The Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Annual Report to Parliament 2000-2001

The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 2001
Cat. No. IP30-1/2001
ISBN 0-662-66226-1

This publication is also available on our Web site at www.privcom.gc.ca

Office of the Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissariat à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Télec.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

December 2001

The Honourable Daniel Hays
The Speaker
The Senate of Canada

Dear Mr. Hays:

I have the honour to submit to Parliament my annual report which covers the period from April 1, 2000 to March 31, 2001, for the *Privacy Act* and from January 1, 2001 to November 30, 2001, for the *Personal Information Protection and Electronic Documents Act.*

The timing of this year's report is exceptional. I had decided to submit the report in early autumn this year rather than in the spring as usual, for two reasons: first, having taken up my position in September 2000, I wanted a sufficient time frame of experience on which to report; and, second, with the *Personal Information Protection and Electronic Documents Act* having come into effect on January 1, 2001, I wanted the report to encompass a reasonable amount of experience with the new legislation. Then the events of September 11, and the privacy issues arising from their aftermath, necessitated waiting until now. The normal reporting schedule of my Office will be resumed with a report next spring.

Yours sincerely,

George Radwanski
Privacy Commissioner of Canada

Office of the Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissariat à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Télec.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

December 2001

The Honourable Peter Milliken
The Speaker
The House of Commons

Dear Mr. Milliken:

I have the honour to submit to Parliament my annual report which covers the period from April 1, 2000 to March 31, 2001, for the *Privacy Act* and from January 1, 2001 to November 30, 2001, for the *Personal Information Protection and Electronic Documents Act*.

The timing of this year's report is exceptional. I had decided to submit the report in early autumn this year rather than in the spring as usual, for two reasons: first, having taken up my position in September 2000, I wanted a sufficient time frame of experience on which to report; and, second, with the *Personal Information Protection and Electronic Documents Act* having come into effect on January 1, 2001, I wanted the report to encompass a reasonable amount of experience with the new legislation. Then the events of September 11, and the privacy issues arising from their aftermath, necessitated waiting until now. The normal reporting schedule of my Office will be resumed with a report next spring.

Yours sincerely,

George Radwanski
Privacy Commissioner of Canada

Table of Contents

Commissioner's Overview 1

Part One – Report on the *Privacy Act* 25

Introduction 25

Investigations 26

Complaints under the *Privacy Act* 26

Definitions under the *Privacy Act* 29

Summary of Select Cases under the *Privacy Act* 30

Personal information found in DND dumpster 30

Personal information destroyed prematurely by HRDC 31

Concerns regarding release of information about groups by Statistics Canada 32

New electronic system at National Defence compromised privacy of thousands 33

Health Canada does not know if it disclosed personal information 34

Information on vessel licences used to assess sales tax 35

No standard for disclosure of personal information to doctors 35

Personal information of refugee claimant disclosed to another claimant 37

Selection boards and hand-written notes 37

Personal e-mail not necessarily private 38

Incidents under the *Privacy Act* 40

Opening mail – right to privacy must be first consideration 40

Health Canada and its list of would-be marijuana users 41

Completed firearms licence applications stolen from Justice Canada 42

Concerns about biometric identification technology 42

Taxpayer received someone else's refund 43

Public Interest Disclosures 43

Privacy Practices and Reviews 52
Introduction 52
Personal documents not shredded – Golden West Document Shredding Inc. 52
Privacy concerns at Canadian Firearms Program 56
New databank protocol in place following Longitudinal Labour Force File 58
Reviews 60
Immigration and Refugee Board, and Canadian Nuclear Safety Commission 60
In the Courts 60
Introduction 60
Recent Decisions 60
Privacy Commissioner v. Canada Labour Relations Board 60
Information Commissioner of Canada (Appellant) v. Commissioner of the RCMP (Respondent) and Privacy Commissioner (Intervenor) 61
Ongoing cases 62
Traveller Declaration Forms (form E-311) 62
Privacy Commissioner v. Attorney General of Canada 62
The Charter Challenge 63
Clayton Charles Ruby v. Solicitor General 64
Office of the Commissioner of Official Languages (Appellant) v. Robert Lavigne (Respondent) 66

Part Two – Report on the *Personal Information Protection and Electronic Documents Act* 67
Introduction 67
Update on Provincial and Territorial Legislation 69
Determination of "Substantially Similar" 69
Consent 69
Reasonable Person Test 69
Access and Correction Rights 69
Oversight 70
Redress 70
Legislative initiatives to regulate the private sector 70
Health Sector 70
Public Sector Legislation 71

Investigations 71

Commissioner's Findings 72

Video surveillance activities in a public place [Principle 4.3, Schedule 1] 72

Unsolicited e-mail from an Internet service provider [Principle 4.3, Schedule 1] 73

Commissioner considers jurisdiction over third-party disclosure by bank subsidiary [section 30] 74

Bank customer requests credit score information [Principle 4.9, Schedule 1, and section 8] 75

Personal information retained after application rejected [Principle 4.5, Schedule 1] 75

Security of a bank's automated telephone service [Principle 4.7, Schedule 1] 77

Musician objects to collection of salary information by professional organization [section 2] 78

Use and disclosure of personal information in telephone directories [Principle 4.3, Schedule 1] 79

Bank teller writes account number on cheque [section 5(3)] 80

Trucking company collects personal information intended for Canada Customs [Principle 4.4, Schedule 1] 81

Bank loses customer's personal information [Principle 4.7, Schedule 1, and section 12(2)] 83

Credit card applicant objects to bank's information-sharing policy 84

Bank accused on withholding bond certificates [Principle 4.9, Schedule 1; and section 8] 84

Selling of information on physicians' prescribing patterns [sections 2 and 3] 85

Estate executor disappointed in search for safety deposit box information [Principles 4.5, 4.9, Schedule 1; and section 8(7)] 87

Employee alleges non-consensual disclosure by employer to investment firm [section 7(3) and Principles 4.3 and 4.5, Schedule 1] 88

Requester alleges non-receipt of credit report from agency [section 8] 89

Airline accused of refusing access to personal information about vacation incidents [Principles 4.1 and 4.9, Schedule 1] 90

Employee objects to employer's use of bank account number on pay statement [Principles 4.3 and 4.7, Schedule 1] 91

Company asks for customer's SIN as matter of policy [Principles 4.3.3 and 4.4.1, Schedule 1; and section 5(3)] 93

User accuses ISP owner of reading and blocking her e-mail [Principle 4.3, Schedule 1] 94

Employer sends third parties copies of response to employee's access requests [Principles 4.3 and 4.5, Schedule 1; and section 5(3)] 95
Telephone company demands identification from new subscribers [Principles 4.2, 4.2.3 and 4.3, 4.3.2, 4.3.3 Schedule 1; and section 5(3)] 97
Broadcaster accused of collecting personal information via Web site [section 2; and Principle 4.3, Schedule 1] 98
Couple alleges bank withheld loan information [sections 8(3) and 8(5)] 99

Incidents under *PIPED Act*
Transportation company collects, discloses passengers' personal information 101
Web site broadcasts cell phone conversations 102

Privacy Practices and Reviews 104

In the Courts 104
Mathew Englander v. Telus Communications Inc. 104
Ronald G. Maheu v. The Attorney General of Canada and IMS Health Canada. 105

Communications and Public Education 106
Public education materials 106
Advertising 107
Web Site 107

Part Three – Corporate Services 109

Gearing up for implementation of the private sector *Act* 109

Corporate Structure 112

102-01861/

Commissioner's Overview

George Radwanski
Privacy Commissioner of Canada

This is my first report to Canadians as Privacy Commissioner. It's a welcome opportunity to look back and take stock of the past year. In just that short time, we've seen extraordinary developments, both technological and social, with unprecedented impacts on privacy. And for me personally, it's been a remarkable year, a voyage of discovery.

I am heartened by the fact that during my brief tenure to date, there have already been several significant victories for the privacy rights of Canadians:

- The federal government's anti-terrorism legislation has been amended to ensure that it encroaches on privacy rights only to the absolute minimum necessary to meet legitimate security objectives. As originally drafted, the legislation contained provisions that went far beyond their stated objectives. They would have given the Attorney General the discretion to deprive Canadians of all privacy protection, by issuing blanket certificates that could effectively have abrogated the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. The Minister of Justice accepted my representations and introduced amendments that fully met my concerns.
- The opening of mail from abroad by customs officers of the Canada Customs and Revenue Agency, on behalf of Citizenship and Immigration Canada, has been restricted to make it much more respectful of privacy rights. The previous practice, based on an arbitrary and outdated weight-based distinction in the *Customs Act* between mail and parcels, was perfectly legal – but it was deeply wrong in terms of privacy. When letter mail was sent in the large courier-type envelopes required by premium delivery services, this alone made it heavy enough to lose the exemption intended to protect the mail of Canadians from being opened without a warrant. Following my discussions with the Minister of National Revenue, he caused the agency to revise its procedures so that the spirit of the law is respected. The outer

envelopes no longer count toward the weight used to distinguish between mail that is entitled to privacy protection, and parcels.

- Deeply flawed provincial "health privacy" legislation in Ontario, which in fact would have given the Ontario government carte blanche to violate health privacy rights, did not go forward. Because our privacy is indivisible – it cannot be respected federally and violated provincially – I accepted an invitation to testify about the proposed law before a committee of the Legislature. Unlike other witnesses who recommended amendments, I suggested that this bill was so fundamentally defective in approach that it would be best to withdraw it and start from scratch. The bill was allowed to die on the order paper. I am hopeful that its eventual successor will be more genuinely aimed at protecting privacy.

These developments give me confidence that the structure of Canadian privacy law, based on an Officer of Parliament/ombudsman with a mandate to oversee the privacy rights of Canadians, is a sound and effective one. With sufficient public support, which depends on presenting the facts cogently and persuasively, much good can be accomplished and much harm can be averted.

I came to this position determined to be an effective champion for the privacy rights of all Canadians. To achieve this, I deemed it necessary both to reinvigorate the Office of the Privacy Commissioner and to greatly increase awareness among Canadians about the privacy issues that affect their lives.

Accordingly, this Office has nearly doubled in size over the past year. When I joined in September 2000 we had 54 people on staff; as of November 30 of this year, our staff had grown to a total of 84 (97 including our corporate services). This was done for two reasons: to meet our new oversight responsibilities under the *Personal Information Protection and Electronic Documents (PIPED) Act* which came into effect in January 2001, and to create a new communications branch which is the key to raising the profile of the fundamental right of privacy.

Public awareness is indispensable to the effective carrying out of my role. As an ombudsman, I basically have two instruments at my disposal: persuasion and publicity. And, of course, persuasiveness is greatly enhanced if it is backed, whenever necessary, by the support of informed, alert public opinion.

Canadians need to know and understand their privacy rights, and to demand that they be fully respected. That is why, since taking office, I have placed great emphasis on my responsibilities as a communicator. I have to date delivered 35 speeches to diverse audiences across Canada, and given more than 210 media interviews.

PRIVACY IS THREATENED AS IT'S NEVER BEEN BEFORE.

Of course, I was aware before I was appointed that privacy is an important issue. I recognized it as a critical element of a free society, and agreed with former Supreme Court Justice LaForest that it was "at the heart of liberty in a modern state." And the argument that privacy is the right from which all freedoms flow – freedom of speech, freedom of association, freedom of conscience, to name just three – struck me as a powerful one.

But it didn't take me long in this position to see that privacy was even more important, and its protection more urgent, than I had realized.

This is a critical time to be Privacy Commissioner. Privacy is threatened as it's never been before. The alarm about "the end of privacy" has been sounded often enough in the past. But it's a sad fact that this alarm was easy for people to dismiss as exaggerated.

A reasonably informed person cannot dismiss it anymore. The technological means to eradicate privacy clearly now exist – not only computers and information processing technology, but also a panoply of technological wizardry from video cameras to facial recognition software to "smart" identification cards. And the motives exist – not necessarily nefarious motives. Indeed, the greatest threats to privacy often come not from those who want to do harm, but from those who argue quite convincingly that privacy must be sacrificed on the altar of some greater good.

Most of us can now easily envisage a world without privacy – not just envision it, but consider it possible and imminent, in a future that we will all live to see. We don't need a George Orwell to say, "Imagine what this would be like." It's beginning to happen all around us.

We're all confronted now with the real possibility of having to go through life with someone looking over our shoulder, either metaphorically or quite literally. We face the real and imminent prospect of having to live our lives weighing every action, every purchase, every statement, every human contact, wondering who might find out about it, judge it, misconstrue it, or somehow use it to our detriment.

That's not freedom. That, on the contrary, is a distinguishing characteristic of totalitarian societies.

Yet I remain concerned that many Canadians are watching but not seeing the assault on privacy. Their attention becomes focused only when their own privacy has already been violated – and by then it's too late. A person's privacy, once violated, can never fully be restored. If personal information about any one of us becomes known by someone who has no business knowing it, there is no way to retroactively make it unknown.

"IF WE REACT TO TERRORISM BY EXCESSIVELY AND UNNECESSARILY DEPRIVING OURSELVES OF PRIVACY AND THE FREEDOMS THAT FLOW FROM IT, THEN TERRORISM WILL HAVE WON A GREAT AND TERRIBLE VICTORY.

The pressures on privacy rights have, of course, become even more acute in the wake of the September 11 terrorist attacks. In a climate of fear and uncertainty, it can become all too easy to believe that the more the state knows about everyone, the safer we will all be. That, in turn, can give an unwarranted new aura of legitimacy to what are precisely some of the greatest threats to privacy – for instance, proliferating video surveillance, widespread use of biometric recognition technology, or national ID cards.

These pressures are further intensified by the fact that a climate of fear not only invites invasions of privacy, it also tends to discourage or penalize dissent. In the face of the destruction wrought by the terrorists, anyone arguing against any measure that has even the vaguest appearance of enhancing security must accept the risk of being accused of irresponsibility.

And yet the world has always been a dangerous place, and the evolution of fundamental rights such as privacy should teach us that their greatest value lies in their ability to endure and protect us in times of the worst adversity. When there is no great incentive to violate a right, it is not so much a right as a fact of life. It is only when the temptation to pursue some goal by brushing everything else aside comes closest to being irresistible, that our society's commitment to protecting fundamental human rights is truly tested.

Privacy and the other cherished freedoms and values that define Canadian society are not frills or luxuries in the situation we face since September 11. They are what this situation is all about. If we react to terrorism by excessively and unnecessarily depriving ourselves of privacy and the freedoms that flow from it, then terrorism will have won a great and terrible victory.

By all accounts, the goal of the terrorist campaign now underway is to attack and undermine the whole nature of American society, and by extension of all democratic societies. That makes our freedoms and values, very much including privacy, the central target. Far from making us safer, every ill-considered reduction of those freedoms – every needless encroachment on privacy – would be a proof that terrorism works and thus an incentive for further mayhem.

My responsibility as Privacy Commissioner is to do everything in my power to help ensure that the fundamental human right, and fundamental Canadian value, of privacy does not in fact fall victim to terrorism.

In discharging this responsibility, I don't argue that privacy is an absolute right, or even that there is no need for privacy-invasive measures to meet the kinds of security threats that we're now facing.

But it is my duty to insist that the choices about any such measures must always be made calmly, carefully, and case by case, and they must be justified according to clear criteria. I have suggested that the following criteria are appropriate, for government and the private sector alike:

- Any proposed measure to limit or infringe privacy must be demonstrably necessary to address a specific problem.
- It must be likely to be effective in addressing that problem – in other words, it must be demonstrable that the measure will make us safer, not just make us feel safer.
- The degree of intrusion or limitation of privacy must be proportional to the security benefit to be derived. It mustn't be a sledgehammer used to kill a fly.
- Finally, it must be demonstrable that there is no less privacy intrusive measure that would achieve the same result.

Though it went through some initial growing pains, the federal government's legislative response to the threat of terrorism is at present, in my view, one that satisfactorily meets these tests with regard to privacy rights. I believe that the new *Anti-Terrorism Act* now strikes a reasonable and careful balance between security and privacy. I am continuing to put forward my concerns and recommendations with regard to subsequent legislation.

Still, there will undoubtedly be further challenges and threats to privacy in the months ahead, in the continuing aftermath of September 11. The choices we make will be of momentous importance.

In the days and weeks following the attacks, the general public got a good look at what privacy advocates have long been worrying about. They saw that there is a huge industry eager to manufacture and sell the technology of surveillance: video cameras, facial recognition systems, fingerprint readers, e-mail and Web monitoring, "smart" identification cards, location tracking. And they saw how many people are eager to argue that if you don't have anything to hide, you shouldn't mind revealing everything.

Over the past year, long before the tragic events of September 11, I have increasingly become convinced that privacy will be the defining issue of this new decade. That is a message I have repeated forcefully in my public appearances. Until recently, what I meant was that we are facing unprecedented and irrevocable choices with regard to privacy because of advances in technology and science, and those choices will determine the quality of our lives.

"I prefer a more modern and refined definition of privacy as the right to control access to one's person and information about oneself.

That remains true. But now more than ever, privacy will be the defining issue, because the choices we make about the balance between security and privacy will determine what kind of society we leave for our children and grandchildren. Even an Orwellian society devoid of privacy wouldn't be entirely secure – the most oppressive police state is still not immune to terrorism – but gradually depriving ourselves of our privacy rights in the name of safety would strip our lives of the dignity and freedom that are the hallmarks of our society.

We will inevitably see this in retrospect as the decade in which we had our chance to take a stand in asserting the crucial value of privacy and defending it against its assailants. I very much hope we will be able to recall it as the decade in which we seized that chance and took that stand.

Most people used to define privacy using some variant of the famous formulation of Samuel Warren and Louis D. Brandeis, as "the right to be let alone." That's still a useful definition, and it certainly captures the visceral sense that people have of the importance of privacy.

I prefer a more modern and refined definition of privacy as the right to control access to one's person and information about oneself. This definition better captures the nature of modern threats to privacy, which take place chiefly in the context of the collection and use of information about us.

That's why I've said so often in the past year that we're at a crossroads. The means by which we protected privacy in the past, or rather the means by which we could leave it to take care of itself, don't work well anymore, and they will work less and less well as time goes on.

Privacy used to be protected pretty much by default. When information about us was in paper records and scattered over many locations, compiling a detailed dossier on any individual was a daunting task. Unless you were famous, important or suspected of a grave offence, your privacy could be relatively safe without your having to make much effort to ensure it.

The move to electronic record-keeping has changed all that, eating away at the barriers of time, distance, and cost that once guarded our privacy. New surveillance technologies – cookies and Web bugs, video cameras, e-mail monitoring, smart cards, biometric identifiers, location tracking, drug testing – assail us wherever we turn. Strangers sitting at computer keyboards compile dossiers on us in seconds. Our activities and our interests, our purchases and our movements, our opinions and our habits are dutifully recorded, analyzed, and classified, for whatever use the highest bidder can dream up for them.

With the default protection vanishing, it's up to us.

> PRIVACY HAS TO BE SEEN, NOT AS A SELFISH INDIVIDUAL INTEREST THAT HAS TO GIVE WAY BEFORE GREATER SOCIAL NEEDS, BUT AS THE SHARED, COLLECTIVE, SOCIAL INTEREST THAT IT IS.

As I mentioned earlier, one of the most interesting things I have observed in the past year is that the greatest threats to privacy seldom come from those who want to do harm.

They come from well-intentioned people who say that privacy needs to be sacrificed for some greater good – improved customer service, prevention of crime, the advancement of science, more efficient delivery of government programs, security.

Of course, sometimes privacy *does* have to yield to other social interests.

But we need to ask ourselves – and ask those well-intentioned people – what kind of society we would be serving, building, and promoting, if the destruction of privacy were too readily the price to be paid.

Privacy has to be seen, not as a selfish individual interest that has to give way before greater social needs, but as the shared, collective, social interest that it is.

That's why it's an important time to be Privacy Commissioner.

It's also an important time to have a new private sector privacy law. For almost 20 years, we've had legislation controlling the way the government collects and handles the personal information of Canadians. It's in the private sector that we are seeing the greatest explosion in collection of information and compilation of dossiers about us. It's there that it's most urgent that we assert control over our personal information.

Parliament passed the *Personal Information Protection and Electronic Documents Act* almost two years ago, and it began coming into effect on January 1st of this year. This *Act* is an important tool for Canadians to reassert control over their personal information, and to take a stand to protect and preserve privacy.

The *Act* applies to personal information collected, used, or disclosed in the course of commercial activities. At its heart is a model code for the protection of personal information, which was developed jointly by business, government, and consumer groups. The code is based on widely accepted principles of fair information practices, including those set out by the Organisation for Economic Cooperation and Development in 1980.

What the *Act* says, in a nutshell, is this:

- Apart from some very limited exceptions, no private sector organization can collect, use or disclose personal information about you without your consent.
- It can collect, use or disclose that information only for the purpose for which you gave consent.

- Even with consent, it can only collect information that a reasonable person would consider appropriate under the circumstances.
- People have the right to see the personal information that is held about them, and to correct any inaccuracies.
- There is oversight, through me and my office, to ensure that the law is respected. And there is redress if people's rights are violated.

The *Act* is coming into effect in stages. It has applied since January of this year to personal information, other than health information, of customers or employees of works, undertakings, or businesses under federal jurisdiction – principally banks, telecommunications, broadcasting, and inter-provincial or international transportation, as well as in the Northwest Territories, Yukon and Nunavut, where it applies to the whole private sector, which, under the constitution, is federally regulated.

It also applies to personal information – again, other than health information – when it's disclosed across provincial or national boundaries for consideration. "Disclosed for consideration" is legalese meaning that you get something in exchange for it – for example, through sale, lease, or barter. The personal information itself must be the subject of the exchange for the *Act* to apply.

The exclusion of personal health information was a last-minute compromise, and it's temporary.

When the law was working its way through Parliament, representatives from the health care sector expressed two distinct, opposite sets of concerns. Some wanted a tougher law, with stronger consent provisions and restrictions on subsequent uses of personal health information. Others argued that the law would constrain operational activities in health care, and wanted it to be more permissive.

But there weren't any fundamental problems or obstacles to overcome. Everyone recognized that personal health information had to be protected. Neither then, nor at any time since, has anyone produced specific, clear indications why the law as written cannot work satisfactorily. In fact, as then-Deputy Minister of Health David Dodge testified before a Senate committee:

> "I have been asking for about six months for some specific examples of things that would really go wrong if the bill comes into effect, as indicated, in a year's time. I have been pressing to determine what things would actually fall down, what we really could not do. Frankly, I have been surprised that despite the general criticism and uncertainty I have not been given examples of things that would go wrong. There is an unease and uncertainty because

PERSONAL HEALTH INFORMATION – INFORMATION ABOUT THE STATE OF OUR OWN BODIES AND MINDS – IS ARGUABLY THE MOST PRIVATE INFORMATION OF ALL.

we are into new territory. However, I have not had examples of things that would actually go wrong."

It was eventually agreed that health information would be excluded from coverage under the *Act* for one year after its coming into force. This was to give the health sector additional time to adapt to the new law.

In recent months, there has been a determined lobbying effort by various powerful health sector interests to continue depriving Canadians of the health privacy protection they were promised would come into effect on January 1, 2002. Some have been pressing for an extension of the exemption or carve-out for personal health information. Others would like to see the law tinkered with in a variety of possible ways, including a separate regulatory regime that would bypass the provisions of the *Act* and truncate the oversight role of the Privacy Commissioner.

But two things have remained constant over the past year. First, there is still no substantive consensus, with some still arguing for a stronger law and others for a weakened one. And, second, no one has yet demonstrated specifically and persuasively what is wrong with the law as written.

Any delay or dilution of the health privacy protection that Canadians have been promised by Parliament would, in my view, be a great blow to privacy rights.

Personal health information – information about the state of our own bodies and minds – is arguably the most private information of all. Any inappropriate disclosure can have devastating consequences. Indeed, fear of losing control over their health information can deter people from seeking medical care at all, with detrimental results not only for them but also for society as a whole. That's why any privacy protection legislation that does not fully protect personal health information is scarcely worthy of the name. The one-year delay in this regard was more than long enough.

An even greater concern would be the effect that any delay or tampering with regard to health privacy protection could have on the effectiveness of the *PIPED Act* as a whole. People in the health field may argue that their sector has special and distinct privacy issues. But people in banking, transportation, telecommunications – indeed, any sector of the economy – could easily make the same argument.

That is why the law was drafted in terms of relatively broad principles and rules, with ample room for flexibility and interpretation in its application. If special exceptions were to be made for one sector such as health, every other sector could likewise start demanding individualized treatment and the whole edifice of the privacy law would be at risk of crumbling.

"IT IS IMPORTANT TO NOTE THAT THE HEALTH CARE SECTOR WILL STILL HAVE ANOTHER TWO YEARS TO PREPARE FOR THE COMING INTO EFFECT OF THE *ACT* IN THE AREAS THAT ARE PRESUMABLY OF GREATEST CONCERN TO IT.

I am therefore very pleased that the Minister of Health, Hon. Allan Rock, confirmed to me in a letter dated September 24:

> "I do not support the creation of a separate regulatory agency to deal with personal health information under *PIPEDA*. The *Act*, as passed by Parliament just over one year ago, is clear that oversight, redress and audit responsibilities rest with the Privacy Commissioner. The Deputy Minister has also made it clear to stakeholders in the Health sector that we are not contemplating amendments to *PIPEDA* to create a separate Agency for the health sector, nor do we support a delay in the application of *PIPEDA* to the health sector."

I very much appreciate this recognition by the Minister of Health, on behalf of his department, of the vital importance of having health privacy protection come into effect as scheduled on January 1, 2002.

At the time of writing of this report, it does indeed appear that the *Act* will apply as written. On January 1, 2002, the personal health information held by federal works, undertakings and businesses about their customers or employees will be protected.

The sale or barter of personal health information across national or provincial borders will also be covered. Disclosures of personal health information across any borders for consideration (where the consideration is for the information) will be covered. And all businesses and organizations in Yukon, the Northwest Territories and Nunavut that collect, use, or disclose personal information in the course of commercial activities will have to protect personal health information as well.

It is important to note that the health care sector will still have another two years to prepare for the coming into effect of the *Act* in the areas that are presumably of greatest concern to it. That's because the *Act* will not apply to such directly health-related commercial services as doctors' offices, private clinics, laboratories and pharmacies until January 1, 2004, when it extends to all private-sector commercial activities within provinces, except where a province has passed substantially similar legislation.

There is, however, one issue that I consider appropriate to address at this time.

I know that members of the health community are understandably concerned about the possible impact of the *Act* on health research, since it involves personal health information and pecuniary considerations are not always absent. I want at this time to provide assurance that bona fide health research, carried out with appropriate sensitivity to the privacy rights of Canadians, has nothing to fear from the *Act* or my Office.

My position on this important issue will be as follows:

Personal health information is perhaps the most privacy-sensitive of all personal information, and as a general rule individuals must have the right to control who can collect, use or disclose this information, and for what purpose. At the same time, however, our society has a vital interest in the continuation and development of health research, which holds the promise of great benefits for all individuals.

The Purpose clause of the *Act* specifies that its rules are intended to balance "the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

In the case of health research, it appears clear to me that the appropriate balance is one that safeguards the genuine privacy interests of individuals while permitting the conduct of legitimate health research that uses information in ways that can have no possible impact on the individuals to whom it pertains. I do not believe that the *Act* was in any way intended to deter or impede such research, and my provincial and territorial counterparts with whom I discussed the issue this summer share this view.

Accordingly, I intend to interpret broadly the intent of paragraph 7(2)(c) of the *Act*, which permits an organization to use personal information without the knowledge or consent of the individual if "it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used." Paragraph 7(3)(f) makes a similar provision for the disclosure of personal information without knowledge or consent.

I will take the view that bona fide health research carried out by duly accredited organizations under appropriate safeguards does in fact constitute statistical or scholarly study or research, whether or not there is an element of pecuniary interest involved. Merely because research into a particular medical condition may receive funding assistance from an outside source that hopes to reap financial benefit from the discovery of an effective new medication, for example, does not, I believe, change its legitimacy as health research from the point of view of privacy rights.

With regard to the impracticability of obtaining consent for such research, I accept the view of the health research community that cost factors and/or the difficulty of obtaining consent from 100 per cent of a

"In short, soon we will have seamless privacy protection in Canada.

target population make it impracticable to obtain individual consent for many health research studies.

The *Act* requires that the information in question must be used in a manner that will ensure its confidentiality. I consider this requirement to be of paramount importance.

I will accordingly take the position that personal health information can be disclosed and used without consent for health research as described above, but only provided that it remains strictly within the confines of the research project and that it can in no way harm the individual to whom it pertains.

Without limiting the generality of the foregoing, I will consider it an absolute requirement that personal health information disclosed and used without consent for health research purposes can under no circumstances whatsoever find its way to the individual's employers, insurers, relatives or acquaintances, governmental or law enforcement authorities, marketers or any other third parties, nor can the individual be contacted as a result of this information by anyone other than his or her own physician or other primary health care provider, as the case may be.

I and my Office will maintain vigilant oversight over this requirement, and any breach of it would be considered, ipso facto, an extremely grave violation of the *Act*.

I am convinced that this approach will fully meet the intent of the *Act*, effectively protect the privacy rights of Canadians, and permit all legitimate health research to proceed without impediment.

The final stage for implementation of the *Act* will be in January 2004. At that time, it will extend to all commercial activities in Canada, with one important exception: where a province has passed substantially similar privacy legislation, the federal government may exempt organizations and activities in the province from the application of the federal legislation, and the provincial law will apply.

Federally regulated businesses in those provinces will continue to be governed by the federal *Act*. So will personal information in all interprovincial and international transactions by organizations in the course of commercial activities.

In short, soon we will have seamless privacy protection in Canada. All of the private sector will be required to comply with the federal law or a substantially similar provincial one.

One of the points about the new private sector legislation that I have made frequently this past year, especially to business audiences, is that it doesn't set Canada apart from the rest of the world. Similar legislation is found in most economically advanced countries worldwide, with the only significant exception being the U.S. Even there, the debate is less

I DECIDED AT THE OUTSET TO PUT A SPECIAL EMPHASIS ON COMMUNICATIONS.

about the principles than about the best means of observing them.

One of the reasons that this kind of legislation is being adopted is that when one country has it, it can only fully protect its citizens' information if the countries with which it trades have similar protections. To promote a better understanding of how we protect privacy in Canada, I have spoken and participated in conferences in Washington, at Harvard University, and in Brussels, Cambridge, and London, and I've engaged in dialogue with privacy and data protection commissioners from around the world.

When I was appointed as Privacy Commissioner, I looked at the situation we were facing: multiple threats to privacy in the name of reasonable social objectives, ever-diminishing expectations of privacy, a complex new law, and a public that, to some degree, seemed so accustomed to having its privacy whittled away that it was in danger of losing sight of privacy's meaning and importance.

Faced with all that, I decided at the outset to put a special emphasis on communications.

One of my first acts as Privacy Commissioner was to establish a new Communications and Strategic Analysis Branch in my Office, with responsibilities for researching privacy issues and reaching out to the public, to inform them and to get their views. And I personally have seized all available opportunities to spread the word, criss-crossing the country to address conferences and meetings and give interviews to the media.

I have also ensured that the public can get accurate, current information from our Web site – for example, my speeches are available there as soon as I deliver them – and in published form. We've made available information packages on a variety of subjects including identity theft, the census, and, of course, how to access personal information and assert your rights under Canada's privacy laws. We've also published extensive guides for individuals and businesses on the new *Act* and how it will affect them.

I do this because it is profoundly important for Canadians to know their rights and to understand the implications of losing their privacy. And the simple truth is that I rely on public support in my role as an ombudsman, which is the primary way I protect Canadians' rights under the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*.

I do not have formal powers to force government institutions and private sector companies to respect people's privacy, or to make amends when they have failed to do so. I can go to the courts in certain instances, of course, but that's never an optimal solution. What I rely on is the power of public opinion. Few people, in government or in business, want to incur the public's wrath. The better informed the public is, the more its opinion will be respected.

"THE PAST YEAR SAW AN UPSURGE IN SURVEILLANCE ACTIVITIES, BY GOVERNMENTS AND THE PRIVATE SECTOR, THAT HAS PUSHED THIS ISSUE FRONT AND CENTRE.

I want to come back now, as I said I would, to some of the specific privacy issues that have preoccupied me this year.

Surveillance – actual visual surveillance – has long been a central concern of privacy advocates. The past year saw an upsurge in surveillance activities, by governments and the private sector, that has pushed this issue front and centre.

Privacy means being able to go about your lawful business without your every move being scrutinized and monitored. While we have to be very mindful of the more subtle privacy threats presented by modern information collection and management, it is imperative that we not lose sight of the gross violation of privacy that surveillance represents.

Video surveillance is everywhere, in public and private spaces. We've become conditioned to being watched and recorded when we enter a bank or a convenience store, move through an airport, or drive through an intersection. And now, alarmingly, we are seeing a growing inclination to monitor us as we walk on the streets of our cities and towns.

People occupying a public space must reasonably expect to be observed by others. But it's one thing to expose yourself to casual glances, or even interested notice, by your fellow citizens. It's another to find yourself under systematic, relentless observation, without cause, by agents of the state.

We haven't yet reached the same point as the United Kingdom, with its ever-increasing network of video surveillance – some two million video cameras, according to a recent report, watching streets, parking lots, housing developments, and shopping centres. Nor have we yet followed the lead of the U.S., where there are already instances of random video surveillance of public gatherings combined with biometric databases, to produce an electronic equivalent of the police line-up – with everyone required to participate, independent of any suspicion of wrongdoing.

But we have seen the installation of video surveillance systems aimed at public streets in Kelowna, B.C. (the subject of a complaint received by this Office), and similar systems are being planned for various other Canadian cities.

And biometric face recognition technology, in Ontario casinos and at Toronto's Pearson International Airport, also made the headlines this year. (In the latter case the headlines turned out to be wrong: my investigation revealed that the RCMP was using biometrics in a reasonable manner. My account of this is in Part One of this report.)

The rationale for surveillance is always the same: it increases security and helps deter crime. That's not something to be dismissed lightly. Whether it's bank robbery or the running of red lights, privacy advocates have no sympathy for people who hide behind privacy as an excuse for wilful violation of society's rules and laws.

But, as someone once said, the only place where a police officer's job is easy is in a police state. We cannot let legitimate concerns about security override a legitimate concern about privacy. If we sweep everyone into the net, if everyone is a suspect whose every movement can be monitored and perhaps recorded, analyzed, and filed away – just in case – we may well have done the utmost to prevent and control crime. But we will have done it at the unacceptable cost of a fundamental human right.

And if the state has no business monitoring the law-abiding nation, the private sector has even less. Yet, this year, a private security company in Yellowknife decided to make public surveillance its business, and aimed its video cameras onto a downtown street. That was enough to trigger a complaint under the *Personal Information Protection and Electronic Documents Act*, which applies to all private sector activities in the territories. My findings are described in Part Two of this report, but suffice it to say that I found that this was a contravention of the *Act*. I think we can all take some satisfaction from the fact that this company acted without the support of the city's officials, police force, or the public, and stopped conducting the surveillance voluntarily when the public reacted negatively.

What is far more disturbing is the situation in Kelowna, B.C. Here the RCMP, acting as a municipal police force, set up a video surveillance camera to continuously monitor and record everyone on a public street. Investigating a complaint that was made to me by the Information and Privacy Commissioner of British Columbia, I found this activity to be a collection of personal information that is in clear contravention of the *Privacy Act*.

But the RCMP is still continuing 24-hour surveillance through the camera, only without continuous recording. This puts it into technical compliance with the *Privacy Act*, which defines personal information as information about an identifiable individual that is "recorded in any form."

As I made clear in my finding, I consider this sort of video surveillance of public places to be an extremely serious violation of privacy rights even in the absence of recording. It is the very presence of video cameras, whether they are recording at any moment or not, that creates the privacy-destroying sense of being observed. As well, if a proliferation of video cameras is allowed to take place, it is virtually certain that function creep will lead inexorably to the linkage of these cameras

"WHAT IS CRUCIAL TO EMPHASIZE IS THAT THERE IS ABSOLUTELY NO EVIDENCE THAT VIDEO SURVEILLANCE ACTUALLY REDUCES CRIME, RATHER THAN MERELY DISPLACING IT TO OTHER LOCATIONS WHERE THERE ARE NO CAMERAS.

with biometric technology. This would eventually make it possible to identify anyone in a monitored public place at any time, or to monitor the whereabouts and activities of any given individual as he or she moves from place to place.

What is crucial to emphasize is that there is absolutely no evidence that video surveillance actually reduces crime, rather than merely displacing it to other locations where there are no cameras. In fact, a spokesman for the RCMP detachment in Kelowna, Corporal Reg Burgess, was reported in *The Vancouver Sun* of June 19, 2001, as stating that such cameras "do, in some circumstances, prevent crime, but they mostly displace crime."

This *Vancouver Sun* article goes on to report: "Burgess added that, by shifting crime away from Kelowna's downtown core into residential neighbourhoods, police will be alerted to criminal activity more quickly by homeowners."

Since my mandate is to oversee privacy laws rather than the laws of common sense, it is probably beyond my purview to comment on this stated RCMP policy of using video cameras to relocate crime from downtowns to residential areas.

However, I met recently with RCMP Commissioner Giulliano Zaccardelli and tried my utmost to persuade him to demonstrate respect for privacy rights by ordering the removal of the Kelowna surveillance camera. In a letter dated November 27, 2001, Mr. Zaccardelli responded:

> "I am satisfied that in the case of Kelowna, the RCMP is acting within the scope of its duty to protect the community based on well articulated public safety concerns. The use of the cameras will prove to be a valuable asset to the community in suppressing criminal activity and making it a safer place to live."

I then asked Commissioner Zaccardelli for the data on which he bases his conclusion that this video surveillance is indeed effective in assisting the RCMP in its duty to protect the community, and particularly for the evidence that the camera in operation since last February is in fact "suppressing criminal activity" and is making Kelowna "a safer place to live." Specifically, I asked Commissioner Zaccardelli for statistics on the number of arrests arising from the use of the camera since last February, and for statistics comparing the overall crime rate in Kelowna during the months the camera has been in operation to the crime rate for the same period last year. He was not able to provide any such information.

I find this deeply disappointing. One would expect the Commissioner of the RCMP, in choosing to reject the strong recommendation of an Officer of Parliament on such an important matter, to base his decision on the

> I respectfully request the assistance of Members of Parliament and Senators in seeking to persuade Commissioner Zaccardelli to rethink his stance on this issue.

clearest factual evidence, not on unsubstantiated anecdotal conjecture, supposition or wishful thinking.

Even more important, one would expect Canada's highest-ranking police officer, the head of our national police force, to want his force to be exemplary in setting the highest standard of respect for privacy rights. It remains my hope that Commissioner Zaccardelli will come around to that view. If he instead retains his current position on this video surveillance, he will regrettably be setting the diametrically opposite example, to be followed by police forces across the country.

The level and quality of privacy in our country risk being struck a crippling, irreparable blow if we allow ourselves to become subjected to constant, unrelenting surveillance and observation through the lens of proliferating video cameras controlled by the police or other agents of the state.

For this reason, I respectfully request the assistance of Members of Parliament and Senators in seeking to persuade Commissioner Zaccardelli to rethink his stance on this issue. I consider this to be a matter of the greatest importance.

Video surveillance is the most obvious means by which we are being watched and monitored in public. But there are others. The location technology being inserted in cell phones can pinpoint a caller's location to within 50 metres. Geographical positioning technology can be used to locate vehicles. Electronic payments systems used on toll roads and bridges can be used to track the movement of vehicles.

So we have moved well beyond the kind of exposure that "going out in public" used to mean. When we are out in public, we are really out in public – nothing, it seems, can remain private any longer.

And, to add to the problem, as the definition of what is public and what is private becomes blurred, the assault on our public privacy extends to domains that we once considered unquestionably private. A growing number of sensory enhancing technologies – chemical sniffers, thermal imaging devices, night vision binoculars, sound wave receptors, portable x-ray devices – allow what goes on in closed, unquestionably private places to "leak" into public space. The infamous Kyllo case in the U.S., where a marijuana growing operation was detected by a thermal imaging device that captured heat transmissions from the house, shows just how blurred the distinction between public and private can be.

Again, privacy advocates are not advocates of crime. We recognize the good intentions of those who want to use surveillance to increase security. But our society can achieve its legitimate aims for security and prevention of crime without throwing away privacy and the fundamental civil liberties that flow from it.

"EMPLOYEES DON'T SIGN AWAY THEIR FUNDAMENTAL HUMAN RIGHT OF PRIVACY WHEN THEY ENTER INTO AN EMPLOYMENT CONTRACT.

These privacy invasive technologies must be confined to very limited and specific situations where the threat to public security is material, significant, and imminent, and they must be subject to prior judicial authorization – warrants, in other words.

Even the extraordinary growth in generalized surveillance of our public selves, by agents of the state, pales when we compare it to the explosion in surveillance of employees both in and away from the workplace. This is an issue that is of increasing concern to me.

As I told a conference in Toronto last April, workplace privacy is one of those issues that has come to the fore because the default protection of privacy no longer does the job. Privacy rights in the workplace are ill-defined because, until now, they have not had to be defined.

Managers have always wanted to ensure productivity and prevent liability. Even before Henry Ford and Frederick Taylor brought us the production line and "scientific management," managers were monitoring, measuring and conducting surveillance of their workforces.

But for a long time technology imposed a benign limitation on this. Workers were able to maintain a core of privacy in their work – just as they can maintain the privacy of their desk drawers, lockers, and personal effects – simply because monitoring and recording could so easily be overloaded with information.

That benign limitation began disappearing as computers became more common. The dream of perfect control and perfect security is, for all intents and purposes, achievable in the workplace, with technology that allows managers to monitor everything that moves and analyze everything that's recorded.

For some, the idea that employees have privacy rights in the workplace is unacceptable, since they are on the employer's time and property and using the employer's equipment. I don't agree. Employees don't sign away their fundamental human right of privacy when they enter into an employment contract. It may come as a surprise to some that a considerable number of judges and arbitrators agree with me on this.

Nonetheless, we've witnessed an extraordinary growth in surveillance in the workplace. This is particularly apparent in the U.S., where there are few privacy laws to protect employees. In January 2001, the American Management Association surveyed 1,627 large and mid-sized companies and found that more than 75 per cent of them videotape their employees or monitor their e-mail, Internet, phone calls, or computer files. This is up nearly 10 per cent from a similar survey last year.

> ELECTRONIC MONITORING SHOULD NEVER BE ALLOWED TO SUBSTITUTE FOR – IT CAN'T SUBSTITUTE FOR – GOOD MANAGEMENT AND SUPERVISORY PRACTICES.

There have been no comparable studies of the extent of employee surveillance in Canada; it's often simply assumed to reflect the situation in the U.S. That may be an incorrect assumption, partly based on a failure to understand the difference in Canadian laws.

And that failure to understand the difference in laws is frequent in Canada. For example, employers often cite potential liability for workplace harassment as a reason to conduct surveillance, especially of Internet and e-mail use. That reflects U.S. legal doctrine, rather than Canadian. In Canada, anti-discrimination legislation only imposes liability on an employer if it has failed to take reasonable steps to prevent harassment. That doesn't mean wholesale electronic monitoring of the workforce. It means having a good harassment policy, training employees, having good anti-harassment procedures in place (such as a harassment co-ordinator and a confidential complaints process), and acting quickly and effectively if harassment does occur – or if there is good reason to suspect it.

The other excuse I hear for wholesale electronic monitoring is the supposed "potential" of Internet connections for time-wasting and misuse of the employer's facilities. I don't accept that we should monitor employees because of a potential for time-wasting any more than we should monitor the law-abiding public because of the potential for one or some of them to commit a crime. Reasonable suspicion of wrongdoing should be the only justification for monitoring and surveillance of a workforce. Electronic monitoring should never be allowed to substitute for – it can't substitute for – good management and supervisory practices. If the only way an employer can know whether employees are working is to monitor them electronically, there's something wrong with his management practices.

The *Personal Information Protection and Electronic Documents Act* limits collection, use, and disclosure of information to "purposes that a reasonable person would consider appropriate." That's an important restriction on monitoring and surveillance in the workplace. Since the *Act*, or provincial legislation very much like it, will be binding on many employers throughout the country very soon, all employers should be looking at it.

I mentioned earlier the privacy implications of pressure for open government and access to government information. This came to a head this year in the attempt by various parties, supported by the Information Commissioner, to get access to the agendas of the Prime Minister.

That the values of openness and access to information could be twisted into such an attack on privacy – agendas are by their very nature private – has been a painful discovery for me. I never thought I would have to find myself opposing access to information. As a former journalist, I am acutely aware of the importance of openness in government. As an actively involved citizen, I have seen how accountability can be enhanced when information is readily available.

But this unquestionably good thing cannot bulldoze everything in its path, or justify a violation of individual privacy. Once again, privacy has to be asserted in all its societal importance, as a fundamental right, so that we don't see it as something that can be traded away every time someone sees it as an impediment to a valid objective.

Fortunately, I'm not alone in my concern about this. The courts have been very clear: open government doesn't preclude protecting fundamental human rights. Access is an administrative right that can enhance democracy. Privacy is a fundamental human right that is the very essence of democracy.

Another important issue is Government On-Line. The move to a seamless electronic interface between the citizenry and various levels of government can be an excellent development, improving the way programs are delivered and making government more efficient and accessible. Every Canadian has a story to tell about being confused as to which department or which level of government is responsible for which service. And many Canadians know the stories, whether true or apocryphal, of the difficulties that can be encountered in trying to get information from government.

But the walls between agencies and programs, within government and across levels of government, are also walls between collections of personal information. Government as a single, centralized body brings with it the prospect of merging databases of information about individuals' interactions with government. That information has been collected for specific uses. When it's held in separate databases specifically for those purposes, it's compartmentalized.

> PRIVACY HAS TO BE BUILT INTO THESE GOVERNMENT ON-LINE PROJECTS FROM THE START.

When those databases are merged, someone with a need to know only one piece of information can have access to lots more. And information can be combined, to reveal new information, leading to detailed profiles of individuals, tracking their activities and their interaction with government. Combine that with the assignment to each Canadian of an authentication, identification, and access device – what the government is calling "e-identities" – and we could find ourselves faced with a surveillance society, and the end of the right to be let alone.

Moreover, delivering services or benefits electronically will depend on private sector involvement. Private sector providers, as components of government delivery systems, could become repositories of vast databases on Canadians. That is cause for concern, given the limited protection of privacy in the private sector, even with the new private sector legislation.

I've addressed many audiences this year on this subject, and undertaken a continuing process of consultation with the Government of Canada. My message is simple enough: privacy has to be built into these Government On-Line projects from the start. That includes doing privacy impact assessments, and consulting with privacy protection agencies at the design stage – not late in the process, when the privacy problems are already locked in.

Again, I am not questioning the motives of the people behind these initiatives. I have no doubt that their intentions are the best. Efficiency is a worthwhile aspiration. But, as I have emphasized repeatedly, efficiency has to be properly understood, as a relation between means and ends – choosing the best means of achieving defined goals. What's critical is how we define the goals. For government, and for society, those goals have to include the preservation and protection of privacy.

Earlier, I touched on the issue of the privacy of health information. It is difficult to emphasize its importance enough.

Governments at both the provincial and the federal level intend to expand the collection and sharing of personal medical information and develop a comprehensive health information system. The intent is laudable – to deliver a consistent standard of care across the country, assessing why people get sick, and determining who is using, and abusing, the system and why.

But the result may be that a person's latest medical check-up has a potential audience of thousands. And because the state of the health care system is such an urgent concern, privacy issues could tend to be disregarded, or at least given short shrift, in the discussion.

Losing control over health information can have devastating consequences. Fear of losing control may discourage people from seeking medical care at all. The prospect of detailed psychiatric assessments finding their way into an insurance administrator's or an employer's hands, for instance, may be enough to dissuade patients from seeking care. Or they may withhold vital information from doctors, prejudicing the effectiveness of treatment and ultimately wasting the resources of the health care system.

Nearly 87 per cent of doctors in a recent survey in the U.S. reported that a patient had asked them to keep information out of their records. Nearly 78 per cent said they had withheld information from their records because of privacy concerns. We have to wonder whether attitudes are similar here in Canada.

For the patient, health information is fundamentally personal and sensitive. It needs the highest level of protection to ensure that it can never be used to the detriment of the individual to whom it belongs.

I remain very concerned about the security of sensitive medical information. Storing medical records electronically may increase the risks of not just a trickle of isolated privacy violations, but a full-scale flood. We've all heard about unintended disclosures of personal health information and security breaches on the Internet.

Take the recent example of the Eli Lilly and Company's unauthorized disclosure of 700 e-mail addresses of people taking Prozac. Eli Lilly had offered patients taking this drug an e-mail reminder service. The privacy breach took place when an e-mail, sent out at the end of June announcing the end of the program, listed all of the e-mail addresses of the people who had signed up for the service. This simple act created a lot of negative publicity for the company and contributed to the debate in the United States about the difficulty of protecting patient records that are stored electronically.

We also now have examples of hackers gaining access to hospital records. Back in December 2000, *The Washington Post* reported that a Dutch hacker had penetrated the patient record system at the University of Washington Medical Center in Seattle. The hacker is said to have downloaded copies of several thousand patient files containing patient names, conditions, home addresses and Social Security numbers. Closer to home, *The Vancouver Sun* reported in August that five pharmacists in

PRIVACY IS NOT AN OPTION, OR A FRILL.
IT IS A FUNDAMENTAL RIGHT.

British Columbia were recently disciplined and fined by that province's College of Pharmacists for spying on the medication records of colleagues, relatives, friends or acquaintances.

So are we, as a society, prepared for the privacy and security breaches that may be coming? Perhaps, at the very least, we should give patients the right to choose whether to have their medical records stored electronically. We recognize that electronic patient files represent great opportunities for quality of care. But we should also recognize that they represent a challenge from the perspective of patient privacy and confidentiality. The opportunities cannot be realized if the challenge is not met.

Indeed, this fact – that the opportunities of the future cannot satisfactorily be realized if the challenge of safeguarding privacy is not met – applies to all the issues with which I deal and which I have been addressing in this overview.

Privacy is not an option, or a frill. It is a fundamental right. The need to respect that right goes to the very heart of all our hopes for progress as a society and as individuals. That's because all meaningful progress is ultimately about improving the quality of our lives – and we must never delude ourselves that we can achieve such improvement if we pursue it, in any field, at the expense of heedlessly sacrificing the right to privacy which is so essential to our freedom and dignity.

Combating that delusion wherever it arises, and averting that sacrifice whenever someone tries to impose it on us, is what the work of my Office is all about. In the following sections of this report, I will provide an accounting of how we have been discharging our responsibilities.

Part One
Report on the *Privacy Act*

Introduction

The *Privacy Act* protects individuals' privacy with respect to personal information held by federal government institutions.

The *Act*, which has been in force since 1983, governs how federal institutions collect, use, disclose and dispose of personal information, and gives people rights to access and request corrections to their personal information. It also sets out my duties, responsibilities and mandate.

As Privacy Commissioner, I receive and investigate complaints from individuals who believe their rights under the *Act* have been violated. I also can initiate a complaint and investigation myself, in any situation where there are reasonable grounds to believe the *Act* has been violated.

First and foremost, I am an ombudsman, and whenever possible, complaints are resolved through mediation and negotiation. But I also have broad powers of investigation under the *Act*. As Privacy Commissioner I can subpoena witnesses and compel testimony and enter premises to obtain documents and conduct interviews. Obstructing one of my investigations is an offence under the *Act*. Although the *Act* does not include the power to order compliance with the *Privacy Act*, I can, however, recommend changes to the way government institutions handle personal information, based on my investigation findings.

As well, as Privacy Commissioner, I have a mandate to conduct periodic audits of federal institutions to determine their compliance with the *Privacy Act*, and again, on the basis of my findings I can recommend changes.

The *Act* requires me to submit an Annual Report to Parliament on the activities of my Office in the previous fiscal year. This current report covers the period from April 1, 2000, to March 31, 2001.

Investigations

My Investigations and Inquiries Branch investigates individuals' complaints under section 29 of the *Privacy Act* (and under section 11 of the *Personal Information Protection and Electronic Documents Act*, which I'll talk about later in the report).

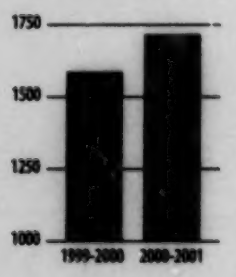
Through these investigations, I determine whether individuals' privacy rights have been violated or whether they've been properly accorded access to their personal information. Where people's privacy rights have been violated, I look for ways to provide redress for them, and prevent violations from happening again.

I have authority under the *Act* to administer oaths, receive evidence, and enter premises where appropriate. I can also examine or obtain copies of records found in any premises.

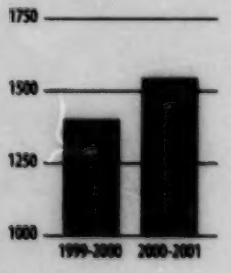
To date, all complaints under the *Privacy Act* have been resolved without our having to use these formal investigative powers, because voluntary co-operation with investigations has been forthcoming.

The Branch also responds to thousands of inquiries from the general public who contact my Office for advice and assistance on all sorts of privacy-related matters.

Complaints Received
April 1, 2000 to March 31, 2001



Complaints Investigations Closed
April 1, 2000 to March 31, 2001



Complaints under the *Privacy Act*

Between April 1, 2000, and March 31, 2001, we received a total of 1,713 complaints under the *Privacy Act*. That's an increase of almost 10 per cent over the previous year. The type of complaints we received conformed to the established pattern: 60 per cent of them concerned either denial of access to personal information or issues of collection, use, disclosure, and disposal of personal information, and the remaining 40 per cent concerned failure to respect time limits, where federal organizations had not responded to a request for disclosure of personal information within the 30-day timeframe set out in the *Act*.

My staff closed 1,542 investigations, an increase of 10 per cent over the previous year. Of the cases closed, 339 dealt with issues of collection, use, disclosure, or disposal, while 630 dealt with access matters and 573 with time limits. These complaints were concluded as follows:

Not well-founded:	421
Well-founded:	553
Well-founded/Resolved:	82
Resolved:	44
Settled during the course of the investigation:	321
Discontinued:	121

Complaints about departments taking longer than they should to respond to access requests are always troubling – justice delayed is justice denied, and the time limits are in the *Act* for a good reason.

Several federal government institutions stand out for particularly often failing to meet the prescribed time frames when responding to individuals' requests for access to their personal information. These are the Correctional Service of Canada, the Department of National Defence, the Canada Customs and Revenue Agency, and Human Resources Development Canada.

I consider it of great importance that all government departments and agencies faithfully meet the time limit requirements set out in the *Privacy Act*. Respecting the lawful rights of Canadians is mandatory, not optional. There simply is no excuse for an entity of the Government of Canada to be breaking a law of Canada, and I intend to keep emphasizing this point.

Correctional Service of Canada

In the fall of 2000, in view of the number of time-limit complaints filed against the Correctional Service of Canada, I instructed my staff to address the matter with senior CSC officials. In February 2001, the Commissioner of Corrections agreed to implement measures to eliminate the backlog of requests in her department.

Those measures resulted in an improvement in the Correctional Service's handling of access complaints. In March 2001, the department had 1,684 active access requests in process, of which only about 20 per cent had been responded to within the prescribed time frame. By August 31, 2001, after an infusion of additional staff and overtime, the department managed to reduce the number of open requests to 501. Nearly 60 per cent of those were responded to within the prescribed time, and 30 per cent were overdue by 30 days or less.

There is no question that this is an improvement, and in July I congratulated the Commissioner of Corrections for her department's achievement. The Correctional Service is continuing to work to reduce the number of outstanding requests and improve its response time. But while I am encouraged by these developments, they are not cause for euphoria. Nothing less would be acceptable.

Department of National Defence

Staff of my office began addressing the issue of timeliness with officials of the Department of National Defence in late 1999. At that time the department had approximately 2,100 outstanding access requests. The great majority of these were not processed within the prescribed time limit. Under pressure from my officials, the department agreed to implement measures such as hiring additional staff, making overtime available, and restructuring its internal procedures and organization.

These efforts have made some difference. As of November 2001, the department had reduced the number of outstanding access requests to 279. Of these, 136, not quite half, were not processed within the prescribed time limits.

Those numbers reflect an improvement, but the situation is still unacceptable. I recognize that, for the most part, the requests concern large files of information pertaining to things like police investigations, Boards of Inquiry, or harassment complaints. Such complaints are difficult to process. But that is a challenge, not an excuse.

Canada Customs and Revenue Agency

This agency has had significant problems responding to access requests in a timely fashion. Staff of my office met with representatives of the agency in early 2000, just as they had done with the Department of National Defence. The agency, just as National Defence had done, agreed to take measures, such as reorganization and hiring new staff, to improve the situation.

In the two fiscal years preceding this one, my office received 81 complaints of failure to respect time limits in one year and 127 in the next. Almost all (95 per cent in one year, 99 per cent in the next) were determined to be well-founded.

This fiscal year, the office received only 61 time limit complaints, and of those, 51 were well-founded.

Although they are better than the previous two years, these figures remain high. Again, the delays probably reflect the complexity of complaints about personal information in tax files, but further improvement is needed.

Human Resources Development Canada

We received 80 complaints against Human Resources Development Canada about failure to respect time limits. Of those, 47 – nearly 60 per cent – concerned access to personal information in the Longitudinal Labour Force File, the "super file" on Canadians that was dismantled last year because of privacy concerns. That was an exceptional situation, given the amount of attention the file received in the media and in Parliament, and the great volume of access requests the department had to deal with. If those exceptional circumstances are subtracted, we are left with 33 complaints about delays in responding to access requests. That number is still too high. But given the number of requests that the department receives in any year, and given the size of this department, the number is small enough to suggest that a bit of reorganization and extra work should suffice to eliminate it. The department needs to do so.

My Office will continue to monitor time-related issues and keep the pressure on for continual improvement.

DEFINITIONS UNDER THE *PRIVACY ACT*

Not Well-founded: A finding that a complaint is *not well-founded* means that the investigation uncovered no evidence to lead me to conclude that the government institution violated the complainant's rights under the *Privacy Act*.

Well-founded: A finding that a complaint is *well-founded* means that the government institution failed to respect the *Privacy Act* rights of an individual. This would also be my finding in a situation where the government institution refuses to grant access to personal information, despite my recommendation that it be released. In such a case, my next step would be to seek a review by the Federal Court of Canada.

Well-founded/Resolved: I will find a complaint to be *well-founded/resolved* when the allegations are substantiated by the investigation and the government institution has agreed to take corrective measures to rectify the problem.

Resolved: *Resolved* is a formal finding that reflects my role as an ombudsman. It's for those complaints where "well-founded" would be too harsh to fit what essentially is a miscommunication or misunderstanding. It means that my Office, after a full and thorough investigation, has helped negotiate a solution that satisfies all the parties.

Settled during the Course of the Investigation: This is not a formal finding but an acceptable means to dispose of a complaint when the investigation is completed, and the complainant is satisfied with the efforts of my Office and doesn't wish to pursue the issue any further. The complainant retains the right to request a formal finding. When that happens, the investigator re-opens the file, and submits a formal report, and I report the findings in a letter to the complainant.

Discontinued: This means that the investigation was terminated before all the allegations were fully investigated. A case may be *discontinued* for any number of reasons – for instance, the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion. I don't issue any formal finding in discontinued complaints.

Summary of Select Cases under the *Privacy Act*

Personal information found in DND dumpster

This case involved files full of personal information found in a trash bin outside an armoury. The files contained the personal information of dozens of Department of National Defence (DND) employees, including their names, home addresses and telephone numbers, dates of birth, medical and dental information, security-screening forms, employment histories, next-of-kin notification forms, performance assessments, and much more.

This information, if disclosed, could have resulted in real harm, and certainly substantial personal and professional embarrassment.

The person who found the files, an army reservist, reported his discovery to senior officers, but no action was taken. He was able to retrieve what he described as a small percentage of the files before the garbage bin was emptied, as usual, at the local dump. He gave the files to my Office and filed a complaint alleging that his personal information had been disposed of in an improper fashion.

My investigation established that an office was being moved to another floor and, in preparation, an order had been given to dispose of anything not needed in the new location. The office held parallel or "shadow files" outside the room where official DND files were kept. Some of the information in these shadow files was a duplicate of official files, some was not. The files were in plain folders without the departmental logo. As they didn't look important from the outside, no one thought to look inside them, and they were simply thrown out as trash.

Mixed in with these plain folders were a number of official DND files that included Candidate Progress Reports with detailed personal information.

Officials at DND reacted quickly, assuring my Office it would implement measures to eliminate the possibility of another occurrence of this nature. The department also agreed to reintegrate information found in the retrieved files into official departmental files.

While the use of "shadow files" does not contravene the *Privacy Act*, I'm very concerned about it. My Office repeatedly finds personal information held in such files throughout federal government departments. Often, the information is not disclosed to individuals seeking access under the *Privacy Act* because it is not maintained in the "official record."

An issue that came up during the course of the investigation was the Treasury Board of Canada guideline on the disposal of personal information.

This guideline describes three levels of personal information. The top level is personal information that, if compromised, "would cause extremely grave injury." Below that is a level that would cause "serious injury" if the information were compromised. The guideline recommends shredding as the method of destroying personal information at these levels.

Below that is what it calls personal information of "low" sensitivity. It defines this as personal information as that which, if compromised, would "cause injury."

According to the guideline, personal information of this type can be torn in half and disposed of in regular garbage containers.

I object strenuously to this guideline and its casual provisions for disposal of information that, by its own admission, could cause injury. I don't accept the distinction it makes between "injury" and "serious injury." Where privacy is concerned, any injury is serious. When personal information of any kind is to be destroyed, it should be shredded.

DND is not the only federal institution following this guideline. My discussions with DND security officials on this matter are continuing.

Personal information destroyed prematurely by HRDC

My investigation into this complaint found Human Resources Development Canada (HRDC) in violation of both the *Privacy Act* and its own Policy Manual.

An Employment Insurance claimant complained to me that his ability to obtain all the information he needed to file an appeal had been hampered by HRDC's destruction of the audiotape of the original hearing into his case by the Board of Referees.

HRDC's Policy Manual stated that such tapes were to be "kept for one year or until such time as the case has been heard by (the Office of) the Umpire, the Federal Court or the Supreme Court, as well, for any re-hearings of the Board of Referees, Umpires, etc." The complainant had been granted two Board of Referees hearings and had appeared before three Umpires (Federal Court judges), but had not exhausted all levels of appeal and was prepared to take the matter to Federal Court and the Supreme Court. Thus, in accordance with HRDC's own policy, the tape should not have been destroyed.

In addition, the *Privacy Act* and Privacy Regulations require government institutions to keep personal information used for an administrative purpose for a period of at least two years, to allow an individual an opportunity to access it.

As a result of my investigation, HRDC agreed to amend its Policy Manual to stipulate a two-year retention for audiotapes of its Board of Referees hearings. It also amended the manual to ensure that staff were aware of the requirements to keep the personal information for two years beyond hearings at every level up to and including the Supreme Court. An instruction was sent out to staff and the Appeals Division issued an amendment to the Policy Manual.

Concerns regarding release of information about groups by Statistics Canada

This complaint raised the interesting issue of "group privacy," which illustrates the need for caution when releasing information about identifiable groups. While disclosures of this kind may not identify any specific individual, they can still have an impact on personal privacy, because information about the group can diminish the privacy of every individual member of the group.

In this instance, a man who had received a series of telephone solicitations from brokerage firms filed a complaint against Statistics Canada, alleging that it had disclosed a sufficient amount of his personal information, obtained from the Canada Customs and Revenue Agency, to enable a research firm to determine his annual income.

The investigation revealed that the information sold by Statistics Canada to the research firm was in fact obtained from the 1991 Census, rather than from income tax records, as the complainant had alleged. And although the information did apply to a specific geographic area, it was not organized by postal code, as the complainant believed it to be. Nor was any of the information about identifiable individuals or personal information as defined in the *Privacy Act*.

In short, Statistics Canada did not contravene the *Privacy Act*. But the complaint did raise an important question about the privacy of members of identifiable groups.

Census products and services, even those based on information gathered from a 20 per cent random sample of the population, can provide a fairly accurate and detailed portrait of the characteristics of the population in a given geographic area. Research companies can and do combine information obtained from Statistics Canada with information obtained from other sources, such as telephone directories and consumer surveys, to compile profiles of specific areas.

When they can identify a relatively homogenous group in a specific geographic area, marketing companies can target individuals in that group, soliciting for everything from financial services to letters from charities.

The potential for damage goes well beyond simple annoyance. Consider the possible effect of a statistical study of a small neighborhood that has a high rate of mental health problems, for example, or a study of an identifiable group that has a high rate of HIV infection.

I have raised this with Statistics Canada. It says that while it makes every effort to ensure that individuals can't be identified in any of its statistical releases, it has established a working group to determine what measures it could take to address issues related to group privacy. It has indicated its willingness to explore this further with my staff. I look forward to further discussions with Statistics Canada on this matter.

New electronic system at National Defence compromised privacy of thousands

Failure to consider the privacy implications of a new electronic information system led to a situation in which any employee of the Department of National Defence (DND) could access personal information on thousands of military personnel. The situation could have been avoided if a few simple safeguards had been put in place.

This case provides a classic example of how easily privacy can be compromised by a well-intentioned attempt at more efficient management.

DND wanted to give managers a tool that would allow them to manage their staff more effectively. However, the project officers neglected to consult the department's privacy co-ordinator to ensure the system respected the requirements of the *Privacy Act*.

As a result, virtually any DND employee could visit the human resources section of the department's internal computer network and read or download detailed personal information about members of the Canadian Forces. This included date and place of birth, home address, marital status, the names and dates of birth of dependents, and results of linguistic testing.

Following the intervention by my Office, DND agreed to take corrective action to end this unjustified disclosure. It transferred the information to a site accessible by password only, with passwords distributed on a strict "need-to-know" basis.

DND also posted an electronic message on the human resources site asking users to destroy any information taken from the old site. I was concerned that this message might not reach all those who may have extracted or downloaded personal information from the file. I asked DND to take an additional corrective measure to trace users. The Assistant Deputy Minister, Finance and Corporate Services, sent a memorandum to all senior managers in National Defence asking them to warn all

employees to destroy any personal information originating from the original human resources site.

It's clear that in this case DND contravened the provisions on the use and disclosure of personal information set out in sections 7 and 8 of the *Privacy Act*, and violated the employees' fundamental right to have their personal information protected. Therefore, I concluded that this complaint was well-founded. Given that DND took satisfactory corrective measures to respect the requirements of the *Privacy Act*, I considered the complaint to be resolved.

Health Canada does not know if it disclosed personal information

An individual complained that a Health Canada doctor inappropriately disclosed his psychiatric assessment to his federal government employer, the Canada Customs and Revenue Agency (CCRA). CCRA had referred the man for a fitness-to-work assessment, which Health Canada does on behalf of federal government departments and agencies. To support his allegation, the complainant referred to a fax cover page indicating that Health Canada had sent an 11-page document to a human resources advisor at CCRA in October 1998.

A check of Health Canada's file confirmed that its doctor had indeed faxed 11 pages to CCRA at that time. However, the complainant's psychiatric evaluation was not found in CCRA's files. It was impossible to determine exactly what Health Canada did send to CCRA or even to confirm whether the fax had reached its intended destination.

If the investigation had confirmed that the evaluation had been sent to the employer, I would then have been required to examine the circumstances of the disclosure. My review would have focused on whether the disclosure met the requirements of the *Privacy Act*.

In this particular case, it is my view that there is a serious records management problem when a federal government department responsible for protecting sensitive medical information cannot determine what documents it sent by fax or whether they were sent to the appropriate individual.

To avoid a recurrence of this problem, Health Canada sent a note to directors of all regional offices reminding them that medical reports should not normally be delivered by fax. In those cases where fax transmission is necessary, it outlined a protocol to be followed in order to keep personal information secure. This protocol includes:

- Identifying the name and telephone number of the recipient;
- Listing contents of the fax on the cover page;

- Contacting the recipient by telephone prior to transmitting the fax to ensure the person is there to receive the document personally; and
- Asking the recipient to confirm receipt of the information in writing.

These principles should be followed by any institution that sends personal information over a non-secure fax line.

Information on vessel licences used to assess sales tax

A man on the West Coast bought a small boat and acquired a small vessel licence issued by Canada Customs officers. He complained that the Canada Customs and Revenue Agency shared the information on his licence application with the British Columbia Ministry of Finance, which proceeded to collect provincial sales tax on the purchase price of the boat. The complainant said he doubted many new boat owners realized their personal information would be disclosed in this way.

While small vessel licences are issued by customs officers, they do so on behalf of the Department of Fisheries and Oceans, which administers Small Vessels Regulations under the *Canada Shipping Act*.

The Department of Fisheries and Oceans' authority to disclose personal information without consent in this way is provided under an agreement between the Governments of Canada and British Columbia, which allows for access, use, and disclosure of personal information to administer or enforce any law. This is consistent with the provisions of the *Privacy Act*, and I concluded that this was a permitted disclosure of personal information without consent.

I did, however, have concerns about the transparency of the collection of the information. The Department of Fisheries and Oceans readily agreed to amend its licence application to advise boat purchasers that their information would be sent to provinces for assessment of sales taxes. The department has also agreed to review the agreement with a view to making it more specific.

No standard for disclosure of personal information to doctors

An individual complained that his employer, the Canada Customs and Revenue Agency, disclosed an excessive amount of his personal information to a psychiatrist.

The individual had presented a claim to the Québec *Commission de la santé et sécurité au travail* for stress-related leave allegedly resulting from the negative work environment created by the employer. The employer contested the employee's claim and requested the opinion of a psychiatrist through Health Canada.

The employer sent a letter to the psychiatrist explaining its concerns about the employee and attached a performance evaluation, which the employee had refused to sign, to support its contentions. The complainant alleged the negative appraisal should not have been disclosed and characterized the disclosure as an attempt by the employer to influence the psychiatrist's opinion.

Health Canada's Protocol for Special Fitness to Work Evaluation states that the employer must give the doctor a description of the problems and the reasons it has requested an evaluation, but says nothing on the issue of sending documents.

The Treasury Board of Canada's Policy on Occupational Safety and Health does not address what type of documentation should be provided to doctors. Nor does Info Source, a directory of federal personal information holdings and the key reference tool in place to assist members of the public in exercising their rights under the *Privacy Act*. Info Source does not address the use of appraisals for the purpose of sick leave or medical opinions. That means federal managers have no directives when it comes to sending documents to doctors performing evaluations on employees. This is not an acceptable situation.

Pursuant to discussions between my Office and representatives of Treasury Board and Health Canada, Treasury Board agreed to revise its Occupational Health Evaluation Standard to include the following directives:

- The employer is required to send the doctor only an explanatory letter.
- The employer must consult the doctor before sending supporting documentation.
- The employer must avoid using and disclosing personal information concerning third parties when submitting its reasons for requesting an evaluation.
- Where circumstances allow, the employer must meet with the employee to explain the reason for the medical opinion, inform the employee what information will be provided to the doctor and why, in order to ensure the transparency of the process.
- The employer must not use or disclose undocumented information such as hearsay or evaluative comments.

Treasury Board has also indicated that it will include this information in bulletins it prepares for the access to information and privacy co-ordinators in federal organizations subject to the *Privacy Act*.

Personal information of refugee claimant disclosed to another claimant

An immigration lawyer complained that the Immigration and Refugee Board disclosed personal information about one refugee claimant to another applicant. What makes this case interesting is that the lawyer was independently representing both clients. The Board gave him the woman's Personal Information Form, which she completed at the port of entry to support her refugee claim, in his role as counsel to the former spouse during his refugee hearing process. The Board notified the lawyer that the woman's form could be used during the spouse's hearing.

The two individuals had arrived at the port of entry together and indicated at that time that they were common-law spouses. The Board argued that the details each claimed were relevant in assessing not only his or her own credibility, but also the credibility of the other. It maintained that the use of this personal information in both claims was consistent with the original purpose of collecting the information, which was to assess their claims for refugee status. I agreed and considered the complaint to be not well-founded.

Nonetheless, this case raises important issues. The lawyer expressed concerns for women, particularly abused women, whose refugee claims are joined with those of other family members. This could mean a woman having to disclose sensitive, intimate details of abuse before a room full of relatives or former relatives. This could be a difficult, traumatic experience, one that would invade the privacy of an individual.

The Board's process does in fact provide for such circumstances. Claimants can make application to have joined claims treated separately. I was pleased to learn that in this case, the Board withdrew the woman's Personal Information Form when the lawyer objected.

The Personal Information Form will also be improved by adding a paragraph that clearly alerts refugee claimants to the possible use of their personal information in another hearing.

Selection boards and hand-written notes

The *Privacy Act* is clear: personal information used by a federal government institution to make an administrative decision about an individual is accessible to that individual, and must be kept for a minimum of two years.

This provision applies to the hand-written notes that members of selection boards take during employment interviews. Members of a selection board ponder their notes in reaching a decision on a particular individual's suitability for a position. That means that the notes have been used for an administrative purpose, and therefore must be retained for at least two years. This issue was addressed in several reports tabled by my predecessor.

In this instance, an unsuccessful applicant for a job with Fisheries and Oceans Canada, in order to prepare an appeal of the competition, requested access to the original, hand-written notes taken by selection board members. The department responded to the request by providing a copy of a typed summary report of its board members notes, and said it had destroyed the original notes upon completion of the competition.

After some deliberation, the department accepted my view that it had a responsibility to maintain its original notes on file. Department officials said there was no deliberate intent to deny access to personal information and assured me that policies have been amended to ensure that the original notes of selection board members are kept on staffing files.

Personal e-mail not necessarily private

A Department of National Defence (DND) employee questioned whether his employer was entitled to use and disclose his private e-mail messages in the investigation of a harassment complaint when those e-mail messages had been collected by improper means.

Someone had gained access to the complainant's computer and downloaded many of his e-mail messages. These messages contained personal information about the complainant, as well as derogatory comments about colleagues. The messages were printed and left on the desks of several employees. After reading the e-mails, these employees gave copies to their supervisor and lodged harassment complaints against the complainant.

The employer hired a consultant to investigate the harassment complaints and gave a copy of the e-mail messages to the consultant as evidence in his investigation. (A separate investigation failed to establish who had downloaded the messages.)

When the complainant learned that his e-mails had been provided to the consultant he complained to my Office, asserting that they had been improperly obtained in the first place, and that the employer had no right to use them in the investigation of the harassment complaints or to disclose them to the consultant.

This case raised important and timely issues. Although this was not a criminal investigation, it nonetheless raised a question about the use in an investigation of evidence that has been obtained unfairly, unethically, and possibly illegally.

That leads us to the whole question of workplace surveillance, and particularly the privacy of e-mail, a very hot topic in the last couple of years. As I mentioned earlier in this report, employers often claim that surveillance of e-mails is justified by the need to protect their employees against harassment.

I firmly believe that employers have to provide this protection. But I don't accept that protection necessarily translates into wholesale surveillance of e-mails or computer use. We accept that there are stringent limits on an employer's right to read employees' mail, eavesdrop on their telephone calls or rifle through their desk drawers. I think we have to look closely at e-mail communications to see what principles should apply there as well.

The Treasury Board of Canada's *Policy on the Use of Electronic Networks* incorporates the principle that the *Charter of Rights and Freedoms* protects employee privacy. It stipulates that institutions must put in place their own specific policy on the use of electronic networks. It further states that the policy should identify authorized and acceptable uses of the networks. The Treasury Board policy does not prevent monitoring if certain conditions apply.

DND's specific policy on the Management of Electronic Mail states that there should be no expectation of privacy on the part of employees when using e-mail systems. I find this deeply troubling. The law on privacy has developed around the notion of the "reasonable expectation"; one of the ways that the courts determine whether privacy has been violated has been to determine first whether a person could have reasonably expected privacy in a particular place and time. But I don't agree that it follows from this that an employee's, or anyone's, privacy can be simply eradicated by telling them not to expect any. While management has the right and the responsibility to manage, it has to operate within limits, including respect for fundamental rights. It is not for management alone to determine whether an expectation of privacy is reasonable.

In this specific case, I concluded that the employer had not contravened any provisions of the *Privacy Act*, and perhaps more importantly that it had not behaved unreasonably in the circumstances. I believe the complainant's expectation of privacy was lost once the e-mail messages had fallen into the hands of colleagues. The rights or wrongs of how that happened were not at issue, as I found no evidence that either the complainant's manager or his supervisor was responsible for monitoring or improperly gaining access to his e-mail.

The employer was authorized to hire a consultant to conduct the harassment investigation, and I concluded that it was authorized to provide the e-mails to the consultant. The e-mails were the basis of the complaints, so the employer could not reasonably have refused to provide them.

Lastly, I advised the complainant that employees who use the employer's electronic network in a manner that contravenes a departmental policy – in this case, to write derogatory messages about co-workers that

could be construed as harassment – should not expect their managers to ignore the inappropriate behaviour when it is brought to their attention. Again, how it was brought to their attention was not the issue. Had there been evidence that managers or supervisors had been responsible for gaining access to the complainant's e-mail, I might well have viewed the matter differently.

Incidents Under the *Privacy Act*

An incident is a matter that has been brought to my attention and warrants an inquiry but is not a formal complaint under the *Privacy Act*. During the period covered by this report, we looked into 21 incidents that came to my attention through various sources. The majority of these dealt with the inadvertent disclosures of personal information or perceived breaches of the *Privacy Act*. The following are some of the more striking examples.

Opening mail – right to privacy must be first consideration

In March 2001, it was revealed that Canada Customs officials were opening mail coming into Canada and passing the information on to Citizenship and Immigration Canada. The sanctity of personal correspondence is a cornerstone of privacy, and Canadians do not expect that their letters sent through the mail will be opened by anyone except the intended recipient. We don't live in one of those countries where mail is routinely opened by the authorities – or so we thought. I immediately looked into this matter.

Many people were surprised to learn that the opening of mail by Customs is lawful, if the mail weighs over 30 grams. If it is less than 30 grams, the *Customs Act* prohibits opening it without either a search warrant or the addressee's consent. But as long as the mail, whether a package or personal correspondence, weighs more than 30 grams, Customs inspectors may open it if they believe that it contains contraband or false documents. Any mail considered suspicious from an immigration standpoint is turned over to immigration officials for examination and further action.

It is of great concern to me that this arbitrary and artificial weight distinction allows the opening of, not just packages, but private correspondence. Correspondence should be treated with the greatest possible respect for privacy. The weight of the correspondence should not make a difference. Sending a letter by any form of "priority post" requires placing it in a large and comparatively heavy outer envelope that by itself can often put the item in the "over 30 grams" category. A letter should not be considered any less "mail," and less deserving of privacy protection, simply because the sender wanted to ensure its timely and safe arrival, or for that matter because it's lengthy and therefore heavier.

I made these concerns known to the Minister of Citizenship and Immigration, and made the following recommendations

- Where Customs officials detect, in an envelope weighing more than 30 grams, a solid object that appears to be something other than correspondence, opening it would fall within the normal activities of the Customs process.
- Where no solid object is detected and an envelope is detained only on suspicion that it may contain fraudulent documents, Customs should pass the mail to Immigration unopened. Immigration could then obtain a warrant to open it if it had reasonable grounds to do so.

The Minister of Citizenship and Immigration rejected the recommendations, citing the apparent difficulty of detecting some solid objects like laminated cards in envelopes, and the great volume of mail passing through a postal facility. Essentially, she argued that implementing the recommendations would demand greatly increased resources.

Since I could not reach a consensus with the Minister of Citizenship and Immigration, I turned my attention to the Minister responsible for the Canada Customs and Revenue Agency. My discussions with the Minister of National Revenue produced a resolution to this matter. Customs has modified its approach and now disregards the weight of courier-type envelopes in determining whether a mailing weighs more or less than 30 grams. Letters within such courier packages are treated as personal mail and not opened if the letters themselves are under 30 grams. I very much appreciate the National Revenue Minister's assistance in resolving this matter.

Health Canada and its list of would-be marijuana users

Health Canada contacted my Office after receiving a call from a newspaper reporter who said she had obtained the names of 128 individuals who had applied to the department for legal exemptions to obtain marijuana for medical purposes.

My investigation focused on two issues: determining the names on the list so that those people could be advised that their personal information had been compromised, and finding out how the list came into the reporter's possession.

The reporter refused to give the list to either my Office or Health Canada. As more than 160 people had applied for the marijuana exemption by the time this matter came to light, there was no way to determine the identities of the 128 people on the reporter's list. Health Canada had no choice but to notify all of the individuals that it had failed to safeguard their personal information.

In order to identify the source of the leak, Health Canada carried out an internal investigation. It found that internal security was not adequate. Virtually all employees in the Office of Controlled Substances had access to the names. Recommendations to improve security were implemented promptly. Now, access to the database is on a need-to-know basis and restricted through the use of passwords.

As for the list itself, following interventions by my Office, the reporter agreed to destroy it. The list has not been published and the reporter confirmed that no copies had been made.

I was satisfied with the security measures implemented by Health Canada and its efforts to sensitize employees to their obligations under the *Privacy Act*.

Completed firearms licence applications stolen from Justice Canada

As part of its efforts to promote firearms registration, Justice Canada's Canadian Firearms Centre runs Operation Outreach, a program to reach the owners of firearms in their own communities. Using storefront operations in malls and vans that travel to small towns and country fairs, staff help people fill out firearms licence applications and mail the completed forms to a licence-processing centre. In British Columbia, one of the vans was stolen. The van was recovered, but a box containing some 20 completed applications that had been in the van was missing.

Following news reports of the incident, I asked that the circumstances of the theft be examined along with the efforts undertaken by the centre to identify and notify applicants whose forms were taken. Not only had personal information gone missing, but that information could be used by unscrupulous individuals to obtain firearms licences they might not be entitled to have.

The centre appealed through the media for individuals to come forward if they had completed an application in the days before the theft. Only two did. The hope remains that other applicants will contact the centre once they realize they have not yet received their licence. As a long-term safeguard, the centre has updated its policy to ensure that completed applications are mailed to the Firearms Centre at the end of each day. Although this incident remains unresolved, I am satisfied with the centre's efforts at damage control.

Concerns about biometric identification technology

Biometric technology, which identifies people by their physical characteristics, is of special interest to my Office. When the media reported that the RCMP was using face recognition software to monitor travellers at Toronto's Pearson Airport and identify criminals, I launched an investigation immediately.

As it turned out, the report was wrong. The RCMP is not using surveillance cameras with biometric software, although the software is in use in the RCMP detention area at the airport to analyze photos of individuals who have been arrested. A photo of the individual under arrest is taken with a digital camera and stored on the hard drive of a stand-alone computer. The software takes point-to-point measurements of facial bone structure and compares this digital portrait of the individual under arrest against those already in the system. As bone structure cannot be altered as readily as hair or eye colour, the system may be able to spot individuals using various identities. This was a sophisticated version of the traditional mug shots used by law enforcement.

In this instance, I was satisfied that biometric software was not being used as the media reports suggested and no privacy concerns were identified.

Taxpayer received someone else's refund

A reporter for the *Calgary Herald* was handed a pretty good story when she received another person's income tax assessment and refund cheque in the same envelope as her own.

An investigation by my Office determined that a mechanical error at Public Works and Government Services Canada's Winnipeg Production Centre was to blame. The Winnipeg Production Centre prints and mails taxpayer assessments and cheques on behalf of the Canada Customs and Revenue Agency.

The plant is fully automated to print, cut, and fold assessments and cheques. The documents are put into envelopes, which are then sealed. The sealed envelopes pass under an optical detector that shines light through them and warns if an envelope is too thick.

This year however, due to changes in the grade of paper used and the number of pages of the form, the envelopes are thicker. The optical detector could not be adapted to accommodate these changes, and was inoperable.

Only one incident of this type has been reported. To help ensure the incident is not repeated, quality control at the plant has been tightened and there is increased random sampling of the final product.

I was satisfied by the steps Public Works took to prevent future errors of this type and by its offer of an apology to the individual involved.

PUBLIC INTEREST DISCLOSURES

Under paragraph 8(2)(m) of the *Privacy Act*, the head of a government department may disclose personal information without the individual's consent where there is a compelling public interest that outweighs the invasion of the individual's privacy or where the disclosure

would benefit the individual. A "compelling public interest" often pertains to public safety and security, or to accountability to the public for decisions taken by departments.

Heads of departments are required under subsection 8(5) of the *Act* to provide me with written notice of any use of this provision. Ideally, this is done prior to the disclosure of the information. If appropriate, I may notify the individual concerned about the release of the information. In all cases, I attempt to ensure that only the minimum amount of personal information needed to achieve the public interest objective is disclosed.

During the period covered by this annual report, I received notice of 53 of these disclosures.

This past year, most notifications came from the RCMP, National Defence, Correctional Service of Canada, and the National Parole Board.

The RCMP made a number of public interest disclosures in relation to the release of sexual offenders into the community at the end of their custodial sentences. In most cases, the individuals' offences had involved children, and they were assessed as being at a high-risk to re-offend. Some had been deemed to be dangerous sexual offenders. Based on concern for citizens in the communities in which the offenders were released, the RCMP deemed the public disclosure of personal information to outweigh the harm caused by the invasion of the offenders' privacy.

On a number of occasions, National Defence disclosed information related to deaths on duty of Canadian Forces members. The information was released to the member's next of kin on compassionate grounds in the hope that a better understanding of the circumstances surrounding the death of their relative would help them achieve some level of closure.

Correctional Service of Canada and the National Parole Board publicly disclosed a number of Board of Inquiry reports dealing with issues such as escapes from federal institutions, breaches of statutory release requirements, and inmates' commission of further offences, including murder, while on release. These reports included personal information. Most of the cases had received significant media coverage. The individuals had been re-incarcerated, but because of the media coverage and the public scrutiny, Correctional Service of Canada and the National Parole Board considered it to be in the public interest to disclose the reports. The public disclosures were seen as necessary for the public to understand the events surrounding the incidents and the actions taken to prevent recurrence.

Top Ten Departments by Complaints Received
April 1, 2000 to March 31, 2001

Organization	Total	Access to Personal Information	Time	Privacy	Other
Correctional Service of Canada	672	136	342	194	
Canada Customs and Revenue Agency	197	91	59	47	
Human Resources Development Canada	190	63	88	39	
Royal Canadian Mounted Police	136	85	24	26	1
National Defence	100	40	46	14	
Citizenship and Immigration Canada	90	32	48	10	
Canadian Security Intelligence Service	40	37	2	1	
Canada Post Corporation	38	16	4	18	
Justice Canada	30	8	12	10	
Foreign Affairs and International Trade Canada	27	4	23	0	
Others	193	97	42	54	
Total	**1,713**	**609**	**690**	**413**	**1**

Completed Investigations and Results by Department
April 1, 2000 to March 31, 2001

Organization	Well-founded	Well-Founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Agriculture and Agri-Food Canada	0	0	0	0	0	5	5
Auditor General of Canada	1	0	1	0	0	0	2
Canada Customs and Revenue Agency	64	15	57	6	28	60	230
Canada Mortgage and Housing Corporation	0	0	0	0	0	1	1
Canada Ports Corporation	0	0	0	2	0	0	2
Canada Post Corporation	5	1	5	0	2	11	24
Canadian Environmental Assessment Agency	0	0	0	0	0	1	1
Canadian Food Inspection Agency	0	0	0	1	0	2	3
Canadian Grain Commission	0	0	0	1	0	0	1
Canadian Heritage	0	0	1	0	0	3	4
Canadian Security Intelligence Service	0	2	43	0	0	2	47
Office of the Chief Electoral Officer	0	0	0	1	0	2	3
Citizenship and Immigration Canada	35	7	21	7	0	12	82
Office of the Commissioner of Official Languages	0	0	0	1	0	0	1
Correctional Service of Canada	262	23	59	48	2	63	457
Environment Canada	0	0	0	0	0	4	4
Finance Canada	1	0	0	0	0	0	1
Fisheries and Oceans Canada	0	0	1	0	0	1	2

Completed Investigations and Results by Department (Continued)
April 1, 2000 to March 31, 2001

Organization	Well-founded	Well-Founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Foreign Affairs and International Trade Canada	3	0	4	1	1	3	12
Health Canada	5	0	26	1	1	2	35
Human Resources Development Canada	79	4	21	14	2	37	157
Immigration and Refugee Board of Canada	4	3	6	0	0	2	15
Indian and Northern Affairs Canada	4	0	2	0	0	5	11
Industry Canada	0	0	5	1	0	3	9
Justice Canada	2	0	43	3	0	8	56
Millennium Bureau of Canada	0	0	1	0	0	0	1
National Archives of Canada	1	0	7	6	2	12	28
National Defence	55	13	26	7	1	26	128
National Parole Board	1	0	3	0	0	7	11
National Research Council of Canada	0	0	2	0	0	0	2
Natural Resources Canada	0	0	0	0	1	0	1
Ombudsman National Defence and Canadian Forces	1	0	0	0	0	3	4
Pension Appeals Board	0	0	0	0	0	1	1
Privy Council Office	0	0	3	1	0	1	5
Public Service Commission of Canada	1	1	3	1	0	0	6
Public Service Staff Relations Board	0	1	5	0	0	0	6

Completed Investigations and Results by Department (Continued)
April 1, 2000 to March 31, 2001

Organization	Well-founded	Well-Founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Public Works and Government Services Canada	8	0	6	1	0	2	17
Commission for Public Complaints against the RCMP	0	1	1	0	0	0	2
Royal Canadian Mounted Police	18	9	51	12	4	25	119
Social Sciences and Humanities Research Council of Canada	0	0	0	0	0	1	1
Solicitor General Canada	0	2	11	1	0	0	14
Statistics Canada	1	0	1	0	0	0	2
Transport Canada	2	0	0	1	0	3	6
Treasury Board of Canada	0	0	3	1	0	0	4
Vancouver Port Authority	0	0	0	2	0	0	2
Veterans Affairs Canada	0	0	3	1	0	13	17
Total	**553**	**82**	**421**	**121**	**44**	**321**	**1,542**

Completed Investigations by Grounds and Results
April 1, 2000 to March 31, 2001

	Well-founded	Well-Founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Access to Personal Information	**11**	**73**	**241**	**54**	**36**	**215**	**630**
Access	11	70	229	51	15	207	583
Correction/Notation	0	3	12	3	21	5	44
Language	0	0	0	0	0	1	1
Inappropriate Fees	0	0	0	0	0	2	2
Privacy	**45**	**9**	**124**	**58**	**8**	**95**	**339**
Collection	3	0	28	33	2	32	98
Retention and Disposal	2	2	9	0	4	7	24
Use and Disclosure	40	7	87	25	2	56	217
Time Limits	**497**	**0**	**56**	**9**	**0**	**11**	**573**
Correction/Time	15	0	1	1	0	0	17
Time Limits	473	0	31	8	0	10	522
Extension Notice	9	0	24	0	0	1	34
Total	**553**	**82**	**421**	**121**	**44**	**321**	**1,542**

Origin of Completed Investigations

April 1, 2000 to March 31, 2001

Province/Territory	Number
Newfoundland	5
Prince Edward Island	3
Nova Scotia	103
New Brunswick	50
Quebec	306
National Capital Region – Quebec	11
National Capital Region – Ontario	177
Ontario	347
Manitoba	82
Saskatchewan	63
Alberta	109
British Columbia	267
Nunavut	0
Northwest Territories	3
Yukon	9
Outside Canada	7
Total	**1,542**

Inquiries by type under *Privacy Act*
April 1, 2000 to March 31, 2001

Subject	Number
Adoption, genealogy, missing persons	31
Census	45
Criminal records, pardons, U.S. waivers	190
E-311 Travel Declaration Form	39
Firearms	44
Longitudinal Labour Force File	68
Medical Records	91
From Members of Parliament	27
No jurisdiction, federal	427
Privacy Act, interpretation and process	6,460
Public Affairs (media, publications)	896
Redirect to provincial commissioners	1,068
Redirect to other federal agency	651
Redirect to other	499
Register of Electors	21
Social Insurance Numbers	746
Other	296
Total	**11,599**

Privacy Practices and Reviews

Introduction

Section 37 of the *Privacy Act* permits me to initiate compliance reviews, at random, of the personal information-handling practices of federal institutions. What this means is that I audit them, to verify whether they are complying with the principles for the collection, use, disclosure, protection, retention, and disposal of personal information set out in sections 4 to 8 of the *Act*.

The Office has been conducting compliance reviews under section 37 since 1984. I have expanded this function during the past year, setting up a Privacy Practices and Reviews Branch, to allow me to assess how well organizations are complying with the requirements set out in the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. (The private sector legislation gives me similar powers of audit; my discussion of private sector audit activity is in Part Two of this report.)

As an ombudsman, I like privacy audits to be non-confrontational whenever possible. An audit, ideally, is a co-operative, constructive approach to dealing with issues before they become complaints. It's useful for organizations that want to improve their personal information-handling practices. Although I have the same powers with respect to audits that I do in investigations – to summon witnesses, administer oaths, and compel organizations to produce evidence – I would only resort to them if I didn't get voluntary co-operation.

My staff in the Privacy Practices and Reviews Branch, in addition to auditing and reviewing, works with federal organizations that are looking for a better understanding of compliance issues and the privacy implications of programs and practices. It's critical for government departments to fully explore how privacy can be protected before they go ahead with plans, however well intentioned, to cut costs or protect citizens. On request, my branch staff reviews new proposals for information management, such as data-matching initiatives, the creation of databases, and information-sharing arrangements with other organizations. This is another way to help ensure that the Canadians' privacy rights are respected.

In the next few pages I describe three key cases concerning the personal information-handling practices of federal institutions.

Personal documents not shredded – Golden West Document Shredding, Inc.

I have spoken many times about the need to develop a "culture of privacy" within organizations, both public and private. Whenever I read a magazine article about privacy, look at a conference agenda, or review the latest survey on people's privacy concerns, the focus is almost always on the private sector. That focus

is appropriate, but we should not lose sight of the enormous diversity of personal information that governments collect, use, and share. In fact, many of the most serious threats to privacy continue to come from governments.

Unlike businesses, governments have the power to demand personal information from their citizens. They collect information using the force of law. When a government agency or program needs personal information to carry out its mission, that information will be collected. Individuals have no choice in the matter.

As citizens, we must interact with government in order to participate in social programs, receive public assistance, and contribute to the public good through taxation regimes. In doing so, we entrust government with some of our most sensitive personal information. Whether applying for employment insurance, filing income taxes, registering firearms, or filling in census forms, individuals are not in a strong position to oppose the collection or use of their information.

So government must be particularly vigilant in maintaining the trust that citizens place in its ability to preserve the security and confidentiality of records that document individuals' lives and their identities as Canadian citizens.

The following finding represents a significant betrayal of that public trust, and provides a glaring demonstration of what can happen when cost and expediency are given precedence over privacy.

More than 30 federal departments and agencies had stored records at the Pacific Region Federal Records Centre of the National Archives of Canada. The centre was holding, literally, tonnes of highly sensitive personal information. The normal procedure is to destroy these records following a required retention period. A *Vancouver Sun* journalist informed us that a private sector company, hired to shred and recycle the records, was instead offering the material for sale to the highest bidder – *intact*, because whole paper brings a higher price than shredded paper on the recycling market.

Investigation revealed that between January and mid-July 1998, the National Archives had sent several hundred tonnes of material to Golden West Document Shredding, Inc. in Burnaby, B.C., for destruction. This was in addition to material Golden West had obtained directly from other federal government institutions. The following partial list catalogues some of the types of records involved and demonstrates the extent to which the privacy of Canadians may have been compromised:

- From Canada Customs and Revenue Agency, more than 22,000 boxes of material including tax returns, T4 slips, statements of investment income;

- From Human Resources Development Canada, claims for employment insurance benefits, employment counselling client files, applications for old age security and guaranteed income supplement;
- From Statistics Canada, census employment records, census interview records, surveys of employment and other surveys;
- From Public Works and Government Services Canada, employee pay records, cheque registers, payroll registers;
- From Citizenship and Immigration Canada, immigration case files.

If this information had fallen into the wrong hands, the consequences could have been disastrous for thousands of Canadian citizens. Detailed personal information, such as social insurance numbers, dates of birth, bank account numbers and home addresses, is a valuable commodity. In the proliferating crime known as identity theft, it is used by criminals to obtain credit cards, open bank accounts, redirect mail, rent vehicles, and even secure employment. Victims of identity theft often incur substantial financial losses, and must expend great efforts to restore their credit and reputation.

My staff found clear evidence that managers at both Public Works and the National Archives knew about the shredding company's serious financial, security, and technical problems before granting it security clearance to transport and shred classified federal paper waste. Moreover, the company that received the shredding contract was not even the same company that had made the original bid. The bid was submitted by "Golden West Document Shredding Inc.", a bankrupt company, and not "Golden West Document Shredding (1995) Inc.", which was awarded the contract. This inconsistency either went unnoticed or was ignored.

The Public Works security officer responsible for inspecting Golden West's facilities concluded that the company was barely meeting minimum requirements to obtain a facility security clearance. But he granted clearance after the manager of the National Archives Federal Records Centre assured him that National Archives would inspect the facility regularly and report any problems to Public Works.

Inspections, as it turned out, were insufficient to prevent the company from selling unshredded classified documents. In July 1998, during a surprise visit to the Golden West shredding facility, employees of Public Works and the National Archives found that approximately 95 tonnes of unshredded classified material had been sold to a paper-buying company, and was baled and prepared for shipment overseas and to the U.S. for recycling.

The RCMP investigated and reported to Public Works, but the report was not made public,

and my office was not informed of this alarming situation. Information we received from the RCMP during our investigation indicated that, before the material was seized at Golden West in July 1998, a recycling company had purchased four truckloads of government information. Two loads had been shipped via truck to the U.S. and another two loads had been shipped overseas, one to South Korea and another to the People's Republic of China. The RCMP was not able to determine whether the material was shredded.

In my findings after investigation, I agreed with the conclusions of the RCMP: responsibility for this incident rested squarely on the shoulders of National Archives and Public Works. Both had failed to exercise proper care in selecting Golden West. Both had failed to carry out their responsibilities to protect the highly sensitive personal information of thousands of Canadians.

The contract with Golden West came about because National Archives had decided to discontinue its in-house disposal service for classified paper waste for government departments. That decision was made in an effort to cut costs. But it was made without paying serious attention to protecting privacy. Monetary savings cannot override the legal obligation to protect individuals' personal information. The National Archives, acting on behalf of other departments and agencies, was fully responsible for the security and confidentiality of all the information until the paper was rendered unreadable. Both the National Archives and Public Works (as the contracting authority) were obligated to ensure the contractor was disposing of the records properly.

The National Archives has a vital role to play in ensuring that classified government records are properly destroyed at the end of their life cycle. It must provide leadership in the setting of standards and practices for records and information management for the Government of Canada. Requiring departments to make their own arrangements for classified waste disposal substantially increases the risks. This incident never would have occurred had the National Archives continued to shred waste at the regional records centre or had federal employees monitored the destruction at all times.

From a risk management perspective, the best solution would be to re-establish on-site shredding of sensitive records by the National Archives. An alternative could be the use of private off-site shredding services, but only if they can guarantee adequate security measures, and only if the shredding is under constant supervision of Archives staff. I understand the substantial resource implications of these options for the National Archives, and I would be prepared to discuss any other equally effective proposals.

Based on the findings of this investigation, I have made a series of recommendations to the National Archives and Public Works, and have requested that they provide my office with a report on how these recommendations will be implemented. I have also asked that in the future they notify my office, without delay, of any accidental or improper disclosure of personal information.

In addition, I have brought my concerns about the security and confidentiality of personal information that is to be destroyed to the attention of the Treasury Board, which is responsible for setting the Government of Canada's Security Policy and ensuring that it is followed by departments. As a result, the Board agreed to carefully examine the recommendations in my report that relate to either the security policy or the particular standard on contract security in the context of the current review of the Security Policy of the Government of Canada with a view to reducing the likelihood of such an incident reoccurring.

Privacy concerns at Canadian Firearms Program

My Office has taken a keen interest in the Canadian Firearms Program since the mid-1990s – naturally, since the program involves the collection and use of large amounts of highly sensitive personal information. The Office identified a number of potential privacy concerns when the concept was first proposed, suggested several changes to protect privacy when the legislation was before Parliament, and provided further comment when the subsequent regulations were attached to the legislation. Not one of our suggestions was accepted.

My Office continues to receive numerous inquiries and complaints about this program, including some from Members of Parliament. My predecessor initiated a review in January 2000 of the personal information-handling practices of the program. That review has now been completed. Based on it, my chief privacy concerns about the program relate to two areas: access and correction rights, and the collection and use of personal information.

The right of access and correction is especially critical because inaccurate or unsubstantiated information in the Firearms Interest Police database, for example, can lead to delays, licence refusals, or unnecessary questioning of neighbours and acquaintances. (The Firearms Interest Police database was created in 1998 to meet the objective of section 5 of the *Firearms Act* with respect to ineligibility to hold a licence. More than 900 law enforcement agencies across Canada feed incident-reporting codes into the National Police Services Network, which then serve as flags in the database during the application-screening process.)

For individuals exercising their right of access to and correction of their personal information held by the Firearms Program, it's proving

to be difficult and time consuming. The multi-jurisdictional nature of the program sometimes results in them having to go from one department or agency, or one level of government to another, to access their personal information.

An individual in a province such as Ontario, for example, where there is provincial and municipal privacy legislation, could be required to submit as many as three separate access requests in order to obtain the personal information related to one firearms licence application submitted at the federal level. The situation is worse for residents of Prince Edward Island, who do not yet have a legislated right of access to their personal information held at the provincial level.

With respect to the collection and use of personal information, my review revealed that the controls limiting access to the Police Information Retrieval System, for example, are inadequate. Firearms officers have access to more information than they need to make decisions about the eligibility of applicants. They also have access to personal information about other individuals, such as witnesses, acquaintances, and victims. These individuals are not applying for licences. The information about them would not normally be relevant to program requirements.

Another problem is that firearms officers rely on information collected from the Police Information Retrieval System database without verifying the accuracy of the information with the originating police agency. This is contrary both to established RCMP policies and to section 6(2) of the *Privacy Act*, which requires that personal information be accurate, up-to-date and complete. The review also revealed that some of the information being collected from police databases for the Firearms Interest Police system relates to incidents that do not qualify under section 5 of the *Firearms Act* or that are based on unsubstantiated information.

I also assessed the personal history questions on the firearms licence application form to determine if they are consistent with the *Privacy Act*'s restrictions on the collection of personal information.

In my view, the Firearms Program has not provided a demonstrable need for all of the questions. I have concerns about the highly intrusive nature of these three questions:

- "19(d) During the past five years, have you threatened or attempted suicide, or have you been diagnosed or treated by a medical practitioner for: depression; alcohol, drug or substance abuse; behavioural problems; or emotional problems?
- 19(e) During the past five years, do you know if you have been reported to the police or social services for violence, threatened or attempted violence, or other conflict in your home or elsewhere?

- 19(f) During the past two years, have you experienced a divorce, a separation, a breakdown of a significant relationship, job loss or bankruptcy?"

I have recommended that questions 19(d) and 19(f) should be eliminated and that question 19(e) should be revised to eliminate the references to "other conflict" and "elsewhere" and to eliminate the ambiguity.

While my review also raised some issues relating to the disclosure of personal information and security measures, I found that the physical, personnel, and information technology security measures are appropriate to the information being protected. But the review revealed that the Firearms Program had not yet implemented policies, procedures and practices with respect to the retention and disposal of program records.

Based on this review, on August 29, 2001, I made 34 recommendations for corrective measures relating to the program's overall personal information management practices. While I have received positive comments from the Royal Canadian Mounted Police, I have yet to receive any response from the Department of Justice.

The review did not address issues that have arisen subsequent to the research and fieldwork that formed the basis of this review, including outsourcing issues and any international information-sharing agreements. In addition, this review did not cover the handling of personal information by the Canada Customs and Revenue Agency. Since January 1, 2001, the Canada Customs and Revenue Agency has been responsible for administering part of the *Firearms Act*, involved in customs declarations and the movement of firearms. At the time of my review, this part of the *Act* was not yet in force. We're currently looking into these aspects of the program.

New databank protocol in place following Longitudinal Labour Force File

Human Resources Development Canada (HRDC) dismantled its Longitudinal Labour Force File in May 2000, after an outpouring of public anger about it. Since then, HRDC has implemented a strict protocol for all future research projects by any of its offices.

The protocol applies to all policy analysis, research, and evaluation activities that require the linkage of separate databanks. It also applies to linking with external data, including activities with an external contractor. It also covers the use of unmasked personal identifiers for survey purposes, whether the survey is conducted by HRDC, a contractor, or Statistics Canada, and whether the source of the data is an internal (i.e., HRDC) or external databank.

Beyond the fact that HRDC will not carry out linkages except for policy analysis and research that are consistent with its legislated mandate, the main feature of the protocol is to seek a balance. It is guided by principles relating to the public interest, including confidentiality, transparency, an assessment of the public good and avoidance of potential harm to individuals and identifiable groups.

I am pleased to see that HRDC recognizes that linking data from separate databases is intrinsically intrusive of privacy. HRDC will only consider such undertakings where the benefits are clearly in the national public interest. Another requirement is that the objective of the project should not be detrimental to the individuals involved or to identifiable groups, in that it cannot be used to make administrative decisions about them.

The protocol also stipulates that the dissemination of information relating to database linkage will be done in accordance with the confidentiality provisions of the *Human Resources Development Act*, the *Privacy Act*, the *Employment Insurance Act*, the *Income Tax Act*, the *Canada Pension Plan* and the *Old Age Security Act*, and with disclosure criteria contained in agreements with the provinces, territories, and other government departments and agencies.

I'm also pleased to see that, among other safeguards, all links among databases will have to satisfy a prescribed review and approval process. This involves the submission of documented proposals to an internal expert committee, the Databank Review Committee, composed mainly of senior HRDC officials. This review process includes consultation with my Office on all such projects, as well as with external partners when the project requires the linkage of HRDC databases with external data. Finally, the recommendation of the Databank Review Committee is forwarded to the Deputy Minister of Human Resources Development, who is responsible for the approval of each project.

HRDC is currently working on a legal protection framework that will govern the future collection and use of data and information obtained from Canadians, to be used by HRDC for its specific research requirements. It will include penalties for misuse and will be done in a manner consistent with federal laws, policies, and procedures, and with the outcomes of any government review of the *Privacy Act*.

Since September 2000, we have provided comments to HRDC on more than a dozen submissions, including the Canada Out-of-Employment Panel Survey, Canada Student Loans Programs-Key Performance Measure, and the Employment Benefits Support Measures Program.

Overall, I am satisfied that, under its protocol for databank linkages and its proposed legal protection framework, HRDC has addressed the concerns that my Office expressed about the Longitudinal Labour Force File.

Reviews

Immigration and Refugee Board and Canadian Nuclear Safety Commission

Reviews of personal information-handling practices under section 37 of the *Privacy Act* were initiated near the end of this fiscal year at the Immigration and Refugee Board and the Canadian Nuclear Safety Commission. These reviews include on-site visits in the National Capital Region and in selected regional offices across Canada. The reviews should be completed during the fiscal year of 2001-2002.

In the Courts

Introduction

My Legal Services Branch, headed by the General Counsel, provides me with specialized legal and strategic advice and litigation support with respect to the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act.*

Section 41 of the *Privacy Act* allows an individual, following my investigation, to apply to the Federal Court for review of the decision of a government institution to refuse access to personal information. From the time the *Privacy Act* came into force in 1983 to March 31, 2001, 106 applications for review have been filed in the Federal Court. Six of these were filed in the past fiscal year.

Section 42 of the *Privacy Act* allows me, following completion of my investigation, to apply to the Federal Court for review of the decision of a government institution to refuse access to personal information, if I have the consent of the individual who requested the information. Three applications have been brought by previous Privacy Commissioners from 1984 to fiscal year end 2001.

Previous Commissioners and I have also intervened before the courts on a total of six occasions from 1984 to the present in applications brought by others, under either the *Access to Information Act* or the *Privacy Act.*

Recent Decisions

Privacy Commissioner v. Canada Labour Relations Board

This was an appeal by my predecessor from the decision of the Federal Court Trial Division. The case centred on notes taken by members of the Canada Labour Relations Board during the hearing of a complaint of a breach of a duty of fair representation. My predecessor argued that the notes, which contained personal information of the requestor, were under the control of the board and therefore subject to a right of access under the *Privacy Act.*

The appeal was heard on May 9, 2000, and the decision was delivered from the bench.

The Federal Court of Appeal held that the board members' notes were not "under the control" of the board for purposes of paragraph 12(1)(b) of the *Privacy Act*. The court stated: "These notes are being taken during the course of quasi-judicial proceedings, not by employees of the board, but by Governor in Council's appointees endowed with adjudicative functions which they must perform not as agent of the board, but independently of other members of the board including the chairperson of the board or a government institution. The principle of judicial independence and its corollary, the principle of adjudicative privilege, as applied to administrative tribunals, lie at the heart of the board's lack of control over the notes as a government institution."

My predecessor did not appeal this decision.

Information Commissioner of Canada (Appellant) v. Commissioner of the RCMP (Respondent) and Privacy Commissioner (Intervener)

This case involved the balance between the *Access to Information Act* and the *Privacy Act*. A list of postings of four named RCMP officers had been requested under the *Access to Information Act*. The Commissioner of the RCMP refused to release the information, on the ground that it related to the employment history of these individuals and was therefore personal information as described in paragraph (b) of the definition of personal information in section 3 the *Privacy Act*. The Information Commissioner applied in court for a review of the refusal.

At issue was whether the information could be disclosed pursuant to paragraph (j) of the definition of "personal information" in section 3 of the *Privacy Act*, which says that information relating to the position or functions of government officers or employees is not personal information.

The Federal Court of Appeal held that the information in dispute was personal information to each officer and was not within the paragraph (j) exception to the definition of "personal information."

The court rejected the RCMP's argument that the exception in paragraph (j) only applies to the current position of a government employee (or to the last position held in the case of a former government employee). The court agreed with the Information Commissioner and myself that paragraph (j) can apply to past positions.

The court rejected the argument of the Information Commissioner that one should take an expansive view of the exception found in paragraph (j) to justify the release of the requested information. The court adopted my position, stating that the exception should be construed in a way that does not allow for the disclosure of an individual's "employment history."

The Information Commissioner has obtained leave to appeal this decision to the Supreme Court of Canada. I will seek to intervene in the appeal.

Ongoing cases

Traveller Declaration Forms (form E-311)

The following two cases concern the disclosure of personal information by the Canada Customs and Revenue Agency (CCRA) to the Canada Employment Insurance Commission for use in an investigative data match program. The personal information in question was taken from Traveller Declaration Forms (E-311 forms) presented to Customs by Canadian residents between 1994 and 1996. The purpose of the data match was to detect employment insurance beneficiaries receiving benefits while out of Canada. The *Employment Insurance Act* requires claimants to be available for work, and disentitles them from receiving benefits if they are absent from Canada.

Privacy Commissioner v. Attorney General of Canada

This is an appeal to the Supreme Court of Canada of a decision of the Federal Court of Appeal. The issues are whether the Federal Court of Appeal erred in finding that the disclosure of "personal information" by Customs to the Canada Employment Insurance Commission was authorized by section 8 of the *Privacy Act* and section 108 of the *Customs Act*, whether paragraph 108(1)(b) of the *Customs Act* provides the Minister with authority to disclose personal information to the Commission for use in an investigative data match program, and whether the Minister properly authorized the disclosure of personal information in the Traveller Declaration Forms to the Commission for use in an investigative data match program.

This was a special case stated for opinion of the Federal Court jointly brought by my predecessor and the Attorney General of Canada. My predecessor was successful before the Federal Court Trial Division but unsuccessful before the Federal Court of Appeal.

The decision of the Federal Court of Appeal was delivered on February 9, 2000, from the bench. The main conclusions are as follows:

- The data match is authorized by the Ancillary Memorandum of Understanding for data capture and release of customs information on travellers entered into on April 26, 1997 by Customs and the Canada Employment Insurance Commission. Paragraph 108(1)(b) of the *Customs Act* gives the Minister of Revenue the discretionary power to authorize the arrangement set out in the 1997 Ancillary Memorandum. An earlier authorization issued in 1991 by the Minister of Revenue under paragraph 108(1)(b) of the *Customs Act* was determined not to be relevant to the matter before the court.
- Paragraph 8(2)(b) of the *Privacy Act* is to be interpreted broadly. The court stated: "In this context, paragraph 8(2)(b) cannot but be interpreted as being a provision that enables Parliament to confer on any Minister (for example) through a given statute a wide discretion, both as to form and substance, with respect to the disclosure of information his department has collected, such discretion, of course, to be exercised in conformity with the purpose of the *Privacy Act*."
- These objectives were met because "the Minister satisfied herself that the disclosure sought by the Commission was for a permissible use and that no more information than that needed by the Commission would be disclosed." In addition, the 1997 Ancillary Memorandum included restrictions on the use of the information and its disclosure to third parties and other measures such as the establishment of an audit trail and provision for destruction of information.

The Charter Challenge

This is an appeal to the Supreme Court of Canada of a decision of the Federal Court of Appeal. The issues are:

- Whether CCRA's disclosure to the Canada Employment and Insurance Commission of personal information from an individual's Traveller Declaration Form, the use of this information in a data match program, and its subsequent use as evidence against the individual, contravenes the individual's right to be secure from unreasonable search or seizure under section 8 of the Charter;
- If so, whether the evidence should have been excluded under subsection 24(2) of the Charter; and
- Whether the provision in the *Employment Insurance Act* which disentitles the individual from receiving benefits while outside of Canada infringes the applicant's mobility rights under subsection 6(1) of the Charter.

The application for judicial review of the decision of the Office of the Umpire appointed under the *Employment Insurance Act* was dismissed by the Federal Court of Appeal. The Federal Court of Appeal, in a decision delivered February 9, 2000, found that there is no reasonable expectation of privacy for Canadians in information contained in E-311 forms such as to engage section 8 of the Charter (right to be secure against unreasonable search and seizure). The court also decided that paragraph 32(b) of the *Unemployment Insurance Act* (now 37(b) of the *Employment Insurance Act:* no entitlement to Employment Insurance benefits while outside Canada) did not go against the freedom of movement guarantee under subsection 6(1) of the Charter.

Status

The applications for leave to appeal to the Supreme Court of Canada in both these cases were granted on August 17, 2000. Both Notices of Appeal were filed and served on August 22, 2000.

Notice of the Constitutional Questions in the Charter Challenge case was served on the Attorneys General of all the provinces and territories as required by the Supreme Court of Canada Rules. The Attorneys General of Ontario, Manitoba and Québec intervened.

These cases were heard on November 7, 2001.

Clayton Charles Ruby v. Solicitor General

This is an appeal to the Supreme Court of Canada of a decision of the Federal Court of Appeal. The applicant was denied access to his personal information in banks maintained by the Canadian Security Intelligence Service. The Solicitor General refused to release the information the applicant had requested. An application for review of the refusals was dismissed by the Federal Court Trial Division. The matter was appealed to the Federal Court of Appeal, where the appeal was allowed in part and two matters were remitted back to the Trial Division for new determination.

Both the Federal Court Trial Division and Federal Court of Appeal considered the constitutionality of section 51 of the *Privacy Act,* which provides for the filing of information *ex parte* with the court and that hearings be *in camera.* Both courts found that the section 2(b) Charter infringement caused by section 51 of the *Privacy Act* is justified under section 1 of the Charter. The issues in the Supreme Court are:

Issues in the Appeal

- Whether section 51 of the *Privacy Act* violates section 7 of the Charter; and if so, whether the violation is justified under section 1; and
- Whether the section 2(b) Charter infringement caused by section 51 of the *Privacy Act* is justified under section 1.

Issues in Cross-Appeal

- Whether the Federal Court of Appeal interpreted paragraph 22(1)(b) of the *Privacy Act* so narrowly that government institutions will not be able to adequately protect the names of sources of information including police informers; and
- Whether the Federal Court of Appeal failed to give adequate consideration to the implications of the "mosaic effect" and the necessity of interpreting the exempting provisions of the *Privacy Act* in such a manner as to preserve the government's ability to protect sources, investigative methods and techniques and the ability to effectively enforce the laws of Canada.

By decision dated June 8, 2000, the Federal Court of Appeal held that section 7 of the Charter was not engaged since the procedural safeguards in section 51 of the *Privacy Act* did not deprive individuals of their liberty interest. On section 2(b) of the Charter, the Federal Court of Appeal held that section 51 of the *Privacy Act* infringed the right to freedom of speech, but could be saved as a justifiable reasonable limit under section 1 of the Charter.

Another issue considered by the court was the proper interpretation of paragraph 22(1)(b) of the *Privacy Act* which permits a government institution to refuse access to personal information where the disclosure could reasonably be expected to be injurious to the enforcement of a law of Canada or a province or the conduct of lawful investigations. The Federal Court of Appeal rejected the argument of the Solicitor General and held that paragraph 22(1)(b) does not authorize a refusal to disclose simply because disclosure could have a chilling effect on the investigative process in general. The notion of injury in paragraph 22(1)(b) does not extend beyond injury to a specified investigation, either actual or to be undertaken.

Status

Mr. Ruby sought leave to appeal to the Supreme Court of Canada from the decision of the Federal Court of Appeal concerning the constitutionality of section 51 of the *Privacy Act*. The Solicitor General sought leave to cross-appeal from the decision of the Federal Court of Appeal regarding the interpretation of paragraph 22(1)(b) of the *Privacy Act*. Both applications for leave were granted by the Supreme Court of Canada on January 18, 2001. I applied for leave to intervene in the issue concerning paragraph 22(1)(b). I was granted leave to intervene on May 25, 2001. I will present arguments before the Supreme Court of Canada that differ from those of both parties.

Office of the Commissioner of Official Languages (Appellant) v. Robert Lavigne (Respondent)

This case is currently under appeal to the Supreme Court. Mr. Lavigne was refused access to his personal information contained in witness statements made in the course of an investigation conducted by the Office of the Commissioner of Official Languages. The Office based its refusal of access on the exemption in paragraph 22(1)(b) of the *Privacy Act*.

Mr. Lavigne applied to the Federal Court Trial Division under section 41 of the *Privacy Act* for review of the Office's refusal. The previous Privacy Commissioner and I intervened in support of Mr. Lavigne throughout this litigation. Our interventions have been successful before both the Federal Court Trial Division and the Federal Court of Appeal.

By decision delivered September 6, 2000, from the bench, the Federal Court of Appeal ordered the Office of the Commissioner of Official Languages to provide Mr. Lavigne with his personal information. The Federal Court of Appeal relied on two of its previous decisions, *Rubin v. Canada (Minister of Transport)* and *Ruby v. Canada (Solicitor General)*, confirming that the paragraph 22(1)(b) exemption can only be invoked where there is evidence of injury to a specific investigation, the exemption cannot be invoked once an investigation has been completed, and one cannot refuse to disclose the requested information on the basis that to disclose would have a "chilling" effect on possible future investigations. The Federal Court of Appeal rejected the argument of the Office of the Commissioner of Official Languages that a different interpretation was justified in this case by the statutory mandate of the Commissioner of Official Languages.

The issues in the Supreme Court are whether the Court of Appeal erred in finding that the access provisions of the *Privacy Act* override the confidentiality provisions of the *Official Languages Act* and whether the decision of the Court of Appeal seriously compromises the Commissioner of Official Languages' ability to enforce the *Official Languages Act*.

Status

The Office of the Commissioner of Official Languages filed an application for leave to appeal to the Supreme Court of Canada. Leave to appeal was granted on April 19, 2001. The Supreme Court of Canada granted me leave to intervene in support of Mr. Lavigne on August 21, 2001. My submissions as an intervener will be filed in early December.

Part Two
Report on the *Personal Information Protection and Electronic Documents Act*

Introduction

The passage of the *Personal Information Protection and Electronic Documents (PIPED) Act* is an important step forward for Canada. It is a clear commitment to protect our fundamental right of privacy, in an age when it is threatened as never before. With technological developments revolutionizing the way we do business and with organizations demonstrating a limitless appetite for personal information, progressive nations around the globe are recognizing the need to safeguard privacy. The *PIPED Act* places Canada firmly in their front ranks.

Part 1 of the *Act* sets out the conditions under which organizations may collect, use, or disclose personal information, and gives individuals rights of access to and correction of personal information held about them by an organization. It also sets out the process by which individuals may lodge a formal complaint when they believe these rights have been violated or that organizations are not in compliance with the law, and the legal remedies available to them.

This part of the *Act* is being implemented in three stages. In the first stage, which began on January 1, 2001, the *Act* applies to personal information, except personal health information, collected, used or disclosed in the course of commercial activities, or about their

employees, by federal works, undertakings and businesses. This includes the banks, the broadcasting industry, inter-provincial transportation companies and the telephone companies.

The *Act* also applies to disclosures of personal information traded or sold across provincial or national borders. In addition, it applies to the entire commercial sector in the Yukon, Northwest Territories and Nunavut, since all local businesses in the territories are considered to be federal works, undertakings, and businesses, and therefore under the jurisdiction of the federal Parliament.

As of January 1, 2002, the *Act* will apply to personal health information for the organizations and activities already covered in the first stage.

Part 1 of the *Act* will be in force across Canada in the provincially regulated private sector as of January 1, 2004, except where a province or territory has enacted legislation that the Governor in Council considers to be substantially similar to the *Personal Information Protection and Electronic Documents Act*. In these cases, the provincial or territorial legislation will apply to intra-provincial collection, use or disclosure of personal information by organizations subject to the provincial law. The federal law will continue to apply to a broad range of interprovincial and international collections, uses or disclosures. That means that as of January 1, 2004, the privacy rights of Canadians will be protected throughout the private sector, either under the federal *Act* or under a substantially similar provincial or territorial law.

As Privacy Commissioner of Canada, I am responsible for overseeing compliance with the rules for the collection, use, and disclosure of personal information set out in Part 1 of the *Act*. I receive and investigate complaints, and, as with the *Privacy Act*, play the role of an ombudsman, attempting to resolve disputes by negotiation. I also may, with reasonable grounds, audit the personal information management practices of an organization.

The powers of investigation granted to my Office under the *Personal Information Protection and Electronic Documents Act* mirror those contained in the *Privacy Act*, although I have a greatly expanded mandate to conduct research into privacy issues, and to promote awareness and understanding of these issues among Canadians.

This is an interim report on activities related to the *Personal Information Protection and Electronic Documents Act* covering the period from January 1, 2001, to November 30, 2001.

Update on Provincial and Territorial Legislation

Determination of "Substantially Similar"

I will interpret substantially similar as meaning equal or superior to the federal law in the degree and quality of privacy protection provided. The federal law is the threshold or floor. A provincial privacy law must be at least as good, or it is not substantially similar.

To be considered substantially similar, any provincial legislation will have to contain, at a minimum, the 10 principles set forth in Schedule 1 to the *Personal Information Protection and Electronic Documents Act.* While we consider all 10 principles of this code to be interrelated and equally important, I am going to comment on five elements of the law as key components in making an assessment of substantially similar: consent, reasonable person test, access and correction rights, oversight, and redress.

Consent

To the extent that privacy is the right to control access to one's person and to personal information about oneself, there is no control without consent and there is no privacy without control.

The requirement for consent must be at the heart of any good privacy legislation. The federal law says that consent must be informed and that the collection, use and disclosure of personal information without the individual's consent may occur only in specified exceptional circumstances.

An organization can only collect, use or disclose personal information about an individual with the individual's consent (except in certain limited circumstances that are set out in the *Act.*)

After collection, personal information can only be used or disclosed for the purpose for which consent was given (except in certain circumstances that are set out in the *Act.*)

Reasonable Person Test

The reasonable person test provides another important check on organizations. The law states that the collection, use, and disclosure of personal information must be limited to purposes that a reasonable person would consider appropriate in the circumstances.

Among other things, this test prevents organizations from using overly broad or vague statements of the purposes for which information is being collected.

Access and Correction Rights

Individuals must have the right to access personal information that organizations have about them and to correct any information that is incorrect (or to have any disagreement noted and provided to any party who received the information).

Oversight

Where an individual is of the opinion that his or her privacy rights have been violated or the privacy law not respected, the individual must have the ability to complain to a fully independent oversight body with the specific mandate to resolve complaints, thoroughly investigate, mediate, conciliate and make recommendations or issue orders. Such an oversight body also must have the full range of investigative powers to seize documents, enter premises, and compel testimony and initiate audits of an organization's practices.

Redress

Following my report to an organization and a complaint, the federal *Act* allows the complainant (or myself directly) to apply for a hearing in the Federal Court of Canada. The complainant or I can ask the court to order the organization in question to correct its information handling practices and make public the steps it has taken to do so. The court can be asked to award damages to the complainant.

Decisions of the Federal Court can be appealed to the Federal Court of Appeal and with leave to the Supreme Court of Canada.

I believe that there must be corresponding redress provisions in any provincial legislation which purports to be "substantially similar".

Legislative initiatives to regulate the private sector

To date, Quebec is the only province in Canada with personal data protection in effect that applies to enterprises operating in the province as defined in its Civil Code. Elsewhere in Canada, two provincial governments – British Columbia and Ontario – have begun to explore legislative options for the regulation of the collection, use, and disclosure of personal information in the private sector. This is in preparation for the January 1, 2004, date for provincial governments to have legislation in place that is deemed by the Governor in Council, through an exemption order, to be substantially similar to the *Personal Information Protection and Electronic Documents Act.*

Health Sector

The provinces of Alberta, Manitoba and Saskatchewan have all passed health-specific privacy legislation. The legislation in Manitoba and Alberta is currently in force. In December 2000, Ontario introduced the controversial Bill 159, the *Personal Health Information Privacy Act.* This bill died on the order paper.

Public Sector Legislation

New Brunswick's *Protection of Personal Information Act* came into force in April 2001. Prince Edward Island's *Freedom of Information and Protection of Privacy Act* received Royal Assent on May 15, 2001, and will come into force in November 2002. With the introduction and passage of these two acts, every province and territory in Canada with the exception of Newfoundland now has statutory protection for personal information held by government departments and agencies.

Investigations

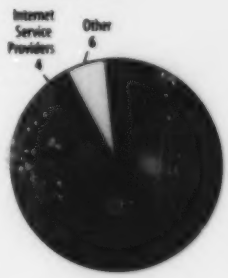
As of November 30, 2001, my Office had received 95 formal complaints under the *Personal Information Protection and Electronic Documents Act*. During this first year of the *Act*, these complaints have been confined to the federally regulated sector, with nearly half of them involving the banks.

In spite of the lead-in time organizations had to prepare for the coming into force of the *Act*, some still have not embraced its principles in their business practices. Many complaints have raised systemic issues dealing with the violation of privacy rights in the federally regulated private sector. Where it was determined that they were well-founded, I have recommended that organizations make important changes to existing policies and procedures.

Section 13 of the *Personal Information Protection and Electronic Documents Act* gives me the authority to ask that organizations report back on the progress made in implementing these changes. Experience to date suggests that this will be a useful tool to ensure the necessary changes are made.

My approach to the investigation and resolution of these complaints is similar to my approach under the *Privacy Act*. When my Office receives a complaint, I give the organization formal notice of the nature of the allegations, and invite it to make representations. I try, whenever possible, to resolve disputes through conciliation, consultation, persuasion and mediation.

Complaints by Sector
January 1, 2001 to November 30, 2001



I may make one of the following findings in handling a complaint:

- **Not well-founded:** This means that there is no evidence to lead me to conclude that the organization violated the *Act*.
- **Well-founded:** This means that the investigation revealed that the organization failed to respect a provision of the *Act*.
- **Resolved:** This means that the organization has taken corrective action to remedy the situation, or that the complainant is satisfied with the results of my Office's inquiries.
- **Discontinued:** This category applies to investigations that are terminated before all the allegations have been fully investigated. A case may be discontinued for any number of reasons – for example, when the complainant is no longer interested in pursuing the matter.

Commissioner's Findings

The following are my findings under the *PIPED Act* up until November 30, 2001. For the sake of consistency, the findings are presented in the format in which they will appear on our Web site at **www.priv- 3m.gc.ca.** Since January 2001 my Office has completed investigations and issued findings and recommendations in the investigation of 27 complaints under the *Personal Information Protection and Electronic Documents Act* and two incidents. Complaints almost identical in nature have been combined and written as one finding.

Video surveillance activities in a public place [Principle 4.3, Schedule 1]

Complaint

The Information and Privacy Commissioner of the Northwest Territories and Nunavut complained that a security company had improperly collected personal information without the consent of individuals by means of surveillance cameras installed on the main street of Yellowknife.

Summary of Investigation

The security company in question had mounted, on the roof of its office building, four video cameras aimed down into a main intersection of Yellowknife and had set up two monitors in its offices. For several days in early May 2001, company staff had monitored live feed from the street 24 hours a day. On several occasions, staff had noted incidents and contacted police. By the company's own admission, this surveillance activity had been a marketing demonstration intended to generate business. On negative publicity, the company removed the cameras less than a week after they had been installed.

Commissioner's Findings (Issued June 15, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because any company in the Northwest Territories is a federal work, undertaking, or business as defined in the *Act*.

Application: Principle 4.3, Schedule 1, states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Since the company's principal reason for installing video surveillance equipment was to monitor the activities of people, the Commissioner concluded that the information at issue was personal information for purposes of the *Act*. Since the company had admitted that its video surveillance activity was a marketing demonstration, the Commissioner concluded that the activity was a commercial activity within the meaning of the *Act*.

The fact that the video feed was live and not taped, was deemed not relevant, since the *Act* does not restrict personal information to recorded information. On the evidence, the Commissioner was satisfied that individuals had not consented to the collection. He found that the company had collected personal information without consent in contravention of Principle 4.3.

In presenting his findings, the Commissioner commented as follows: "There may be instances where it is appropriate for public places to be monitored for public safety reasons. But this must be limited to instances where there is a demonstrable need. It must be done only by lawful public authorities and it must be done only in ways that incorporate all privacy safeguards set out by law. There is no place in our society for unauthorized surveillance of public places by private sector organizations for commercial reasons."

The Commissioner concluded therefore that the complaint was well-founded.

FURTHER CONSIDERATIONS

No further action was required in respect of the complaint, since the company had already removed the cameras before the Commissioner issued his findings. However, the matter was not fully resolved, in that the security company indicated an intention to pursue its efforts to provide video surveillance services to the Yellowknife community. The Commissioner has advised the company that its intended public video surveillance for commercial purposes is unlawful and should not be pursued.

Unsolicited e-mail from an Internet service provider [Principle 4.3, Schedule 1]

Complaint

A customer complained that her Internet service provider (ISP) was using her personal information, namely her e-mail address, without her consent by sending unsolicited e-mail notices to her.

Summary of Investigation

The complainant had received several unsolicited e-mail notices from her ISP about its services. At first she complained directly to the ISP, but was not satisfied with the company's suggestion that she simply reconfigure her browser so as to route the notices directly to a bulk-mail or trash-bin folder. Her position was that the onus should not be on the user to filter unsolicited e-mail notices from the ISP. The company's position was that it had a right to send such messages under the terms and conditions of its subscriber agreement, which contains a consent clause.

Since the initial one-year subscription had been a gift from a friend, the complainant had not personally considered these terms and conditions at the start of her service, but had subsequently been presented with them on renewing her subscription after a year. The complainant did renew her subscription with the same company even though her complaint remained unresolved at the time.

Commissioner's Findings
(Issued July 3, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because Internet service providers are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Principle 4.3, Schedule 1, states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

On reviewing the subscriber agreement of the ISP in question, the Commissioner was satisfied that the company's practice of sending periodic e-mail notices to customers was clearly outlined in the agreement. Hence, he considered it reasonable that customers would expect to receive such notices from time to time. Moreover, he determined that the complainant had consented to the practice on renewing her subscription. He found that in this case the ISP had not contravened Principle 4.3.

The Commissioner concluded therefore that the complaint was not well-founded.

Further Considerations

The Commissioner informed the complainant that he considered the ISP's initial proposal for resolving her concern to have been reasonable. He also commented: "The e-mail notices are in keeping with the purposes for which consent to use the e-mail address was originally obtained, that is, to enable efficient ISP service."

Commissioner considers jurisdiction over third-party disclosure by bank subsidiary [Section 30]

Complaint

A customer complained that an investment company, a subsidiary of a chartered bank, had improperly disclosed to a third party, namely a regulatory body that oversees the company's activities, his personal information related to financial transactions.

Summary of Investigation

The investigation in this case was limited to the Commissioner's determination of whether or not he had jurisdiction in the matter.

Commissioner's Findings
(Issued July 19, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies strictly to federal works, undertakings, or businesses and to transborder disclosures of personal information for consideration. Banks are federal works, undertakings, or businesses as defined in the *Act*. In this case, however, the investment company, though a subsidiary of a bank, operates as a separate and distinct legal entity, does not disclose information across borders for consideration, and is provincially

regulated. The company in question is not currently subject to the *Act*.

The Commissioner concluded that he lacked jurisdiction.

Bank customer requests credit score information [Principle 4.9, Schedule 1, and section 8]

Complaint

A customer complained that a bank had denied her access to her personal information regarding her credit score.

Summary of Investigation

The complainant had telephoned her branch of the bank in question and asked for her credit score information. A customer service representative at the branch advised her that the bank did not release such information to its customers. On being informed of this complaint, the bank undertook an extensive search of its records and subsequently reported that it could not find any credit product or credit application in the complainant's name and therefore had no corresponding credit score for her. The complainant subsequently confirmed that she had no credit products with the bank and had never submitted any credit application to the bank.

Commissioner's Findings (Issued July 23, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because financial institutions are federal works, undertakings, or businesses as defined in the *Act*.

Application: Principle 4.9, Schedule 1, states that upon request an individual must be informed of the existence, use, and disclosure of his or her personal information and be given access to that information. Section 8 sets out conditions under which a request may be deemed to have been refused.

The Commissioner was satisfied that the requested information did not exist in the bank's files. He found therefore that the complainant had not been denied a right of access to her personal information under section 8 of the *Act*.

The Commissioner concluded that the complaint was not well-founded.

Personal information retained after application rejected [Principle 4.5, Schedule 1]

Complaint

A credit card applicant complained that, after turning down her application, a bank had refused her request that the personal information collected for her application be deleted from the bank's records.

Summary of Investigation

The complainant had applied in person for a credit card, but the bank in question had declined her application. The complainant then requested that the personal information

she had provided in her application be removed from the bank's computer system. The branch manager replied that he himself did not have the delegated authority to remove the information, and he took no steps to determine whether some other course could be taken.

In fact, the bank's corporate privacy officer and the business manager for the credit cards had the delegated authority for removal of such information on special request, but in this case the complainant's request was not relayed to either of these officials. For credit card applications made in person, the bank's usual practice was to enter the personal information collected immediately into the computer system at the branch and then forward it for adjudication to the host computer system of the bank's central loan processing centre. If the application was declined, the information was not automatically purged. Unless the unsuccessful applicant made a special request for removal, the personal information remained in the bank's computer system and was accessible indefinitely at the branch level.

Commissioner's Findings (Issued July 23, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because banks are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Principle 4.5, Schedule 1, states that personal information must be retained only as long as necessary for the fulfillment of the purposes for which it was collected.

The Commissioner considered it unreasonable that, after the bank had used the complainant's personal information for the purpose for which it had been collected (i.e., making the decision about the credit card), the information would have remained accessible indefinitely at the branch level had the complainant not insisted on its removal. He found that the bank in this case had contravened Principle 4.5.

However, the Commissioner also noted that the bank had subsequently deleted the complainant's personal information and had confirmed that it had not been communicated to any third party. He also noted that the complainant was satisfied with this resolution.

The Commissioner concluded therefore that the complaint was well-founded and resolved.

Further Considerations

To address the inconsistencies revealed by the Commissioner's investigation, the bank in question has agreed to undertake an extensive review of its current practices for the retention of personal information. The bank has also agreed to implement a communications strategy for educating employees and customers on the bank's privacy complaints process.

Security of a bank's automated telephone service [Principle 4.7, Schedule 1]

Complaint

Citing several provisions of the *Personal Information Protection and Electronic Documents Act*, an individual complained that a bank was not taking adequate security measures to safeguard customers' information disclosed via its automated telephone service.

Summary of Investigation

The bank in question offers an automated telephone service for Visa customers who do not have other dealings with the bank. Users of this service cannot conduct transactions, but can gain limited access to their Visa account information by providing the 16-digit Visa account number and, at the random selection of the system, either the last four digits of the cardholder's home telephone number or the cardholder's year of birth.

Commissioner's Findings (Issued July 23, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because banks are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Principle 4.7, Schedule 1, states that an organization must protect personal information by security safeguards appropriate to the sensitivity of the information.

On consideration, the Commissioner deemed the complainant's concern to be valid. He determined that a coding procedure relying so much upon a cardholder's telephone number or year of birth was not adequate to prevent unauthorized persons from gaining access to users' sensitive personal information. He found that the bank in question was not in compliance with Principle 4.7.

Nevertheless, the Commissioner noted that the bank had proposed and initiated a detailed three-phase action plan to address the security concerns raised in the complaint. He also noted both he and the complainant found all aspects of this plan satisfactory.

The Commissioner concluded therefore that the complaint was well-founded and resolved.

Further Considerations

The action plan proposed by the bank comprises three-phases as follows:

Immediate: All automated access to the complainant's Visa account is disabled, so that any unauthorized attempt to obtain the complainant's personal information will fail. The complainant himself will be able to access his account through an agent by reference to a preselected password.

Short-term: By October 31, 2001, the bank's Visa-only customers will be allowed to disable their automated telephone access upon request and likewise deal directly with an

agent, if they so choose. This phase includes a communications strategy for informing the customers.

Long-term: The bank has agreed to implement a new telephone bank solution addressing the privacy and security concerns of customers within three years and to report on progress to the Privacy Commissioner no later than July 31, 2002.

The Commissioner has commented: "I am satisfied that the measures [the bank] has put in place to resolve the security safeguard issues identified … are acceptable."

Musician objects to collection of salary information by professional organization [Section 2]

Complaint

A musician complained that the professional organization representing his interests had, without his consent, collected personal information about him, namely his annual salary, from his employer.

Summary of Investigation

The complainant is the only musician working in a certain establishment. One of the activities of the professional organization in question is to collect copyright dues for its members, subject to the requirements of the *Copyright Act*. In order to file the applicable tariff with the Copyright Board and collect the copyright dues, the organization first needs to know the total entertainment budget of a given establishment. The complainant was concerned that, since he was the only musician at the establishment in question, a third-party might be able to identify him as the sole recipient of the salary allotment included in the entertainment budget. However, in collecting such information, the organization has no interest in knowing which musicians or how many are working in the establishment and therefore does not collect names or numbers. Nor does it publish or communicate to third parties the information it collects in respect of the establishment.

Commissioner's Findings (Issued July 23, 2001)

Jurisdiction: The professional organization in question stated that it was subject to the *Personal Information Protection and Electronic Documents Act*. The Commissioner did not dispute this position.

Application: Section 2 of the *Act* defines personal information to be "… information about an identifiable individual …".

On the evidence, the Commissioner was satisfied that the professional organization had the legal authority to collect the information at issue and that the collection did not involve personal information about an identifiable individual. He found that the collection was therefore not subject to the requirements of the *Act*.

The Commissioner concluded that the complaint was not well-founded.

FURTHER CONSIDERATIONS

In conveying his findings, the Commissioner commented: "Having established that the information collected is not personal, I need not make a finding on its appropriateness with respect to sections 4.3 (consent) and 4.4 (limiting collection) of Schedule 1 or to section 7 (collection without knowledge or consent) of the *Act*, which might otherwise have applied in this case."

Use and disclosure of personal information in telephone directories [Principle 4.3, Schedule 1]

Complaint

Citing several provisions of the *Personal Information Protection and Electronic Documents Act*, an individual complained that a telecommunications company was:

1. Using and disclosing customers' personal information without their knowledge and consent by publishing names, addresses, and telephone numbers in the company's white-pages directory and on two Web sites; and

2. Inappropriately charging customers for opting not to have their information published.

Summary of Investigation

The telecommunications company in question publishes customers' names, addresses, and telephone numbers in its white-pages directory and on its own directory assistance Web site. In accordance with Canadian Radio-television and Telecommunications Commission (CRTC) regulations, the company gives the same information to the Bell Canada subsidiary that operates the "Canada 411" Web site. Customers are asked how they wish their personal information to appear in the company's white pages and are given the option of not having their information published. For those who choose non-publication, the company charges fees, in accordance with CRTC regulations. The company also provides list services to selected organizations for a fee, excluding information on non-published customers and customers who ask to be de-listed.

Commissioner's Findings (Issued August 14, 2001)

JURISDICTION: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because telecommunications companies are considered to be federal works, undertakings, or businesses, as defined in the *Act*.

APPLICATION: Principle 4.3, Schedule 1, states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

On the matter of consent, the Commissioner considered relevant the company's questioning of customers regarding how their information should appear in the white-pages directory.

He determined that the question itself implies the eventual appearance of the information in publicly available directories. By choosing not to take the option of non-publication, customers implicitly give consent for their personal information to be made available to the public. Moreover, since the information subsequently published in other formats merely reflects what is published in the white-pages directory, it too is considered publicly available information for purposes of the regulations under the *Act* and may be collected, used, or disclosed without consent. In sum, the Commissioner found that the company did obtain valid consent and was in compliance with regulations on publicly available information.

On the matter of charging fees for non-publication of customers' information, the Commissioner noted that the company had duly applied for and received permission from the CRTC, under Telecom Order 98-109, which states that telecommunications companies can charge no more than $2 per month for non-published telephone service. He founded therefore that the company in question did have authority to charge its monthly fee of $2 for non-publication.

The Commissioner concluded that the complaint was not well-founded.

Bank teller writes account number on cheque [Section 5(3)]

Complaint

An individual complained that a bank had created the potential for an improper disclosure of his personal information to a third-party without his consent when a teller wrote his account number on the back of a cheque when cashing it.

Summary of Investigation

The complainant had gone to a branch of his bank to cash a personal cheque from a third party. The bank teller wrote the complainant's account number on the back of the cheque. The complainant's concern was that, if the cheque was for any reason returned to the third party who had written it, the account number would be disclosed to that person.

The bank argued that, in cashing cheques, banks are in effect extending credit until such time as the cheque's value can be debited from the cheque-writer's account. In cases of exception (e.g., fraud or insufficient funds), banks require an efficient means of recovering the cheque value from the customer who presented the cheque. Moreover, names written on the front of cheques are not an efficient enough means, in that they may vary significantly from the exact names in which customers' bank accounts are registered. This bank's position was that recording account numbers on cheques is a longstanding industry-wide practice, necessary for protecting

a bank's interests in ensuring that it can collect its money from either the cheque-writer or the person who deposits or cashes the cheque.

Commissioner's Findings (Issued August 14, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because banks are federal works, undertakings, or businesses as defined in the *Act*.

Application: Section 5(3) states that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

The Commissioner determined that the bank's recording of the account number at the time a cheque is presented is a reasonable practice and that it is reasonable for a customer to expect such practice. The Commissioner was satisfied that the complainant had thus given implied consent to the collection, use, and disclosure of his personal information. The Commissioner found that no contravention of the *Act* had been established.

He concluded therefore that the complaint was not well-founded.

Further Considerations

In presenting his findings, the Commissioner commented as follows: "Upon presenting the cheque for negotiation, the [bank's] customer is giving implied consent for the disclosure of the personal information on the back, just as the drawee is providing express consent to disclosure of their personal information (on the front of the cheque) to the payee."

Trucking company collects personal information intended for Canada Customs [Principle 4.4, Schedule 1]

Complaint

A dismissed employee complained that his former employer, an international trucking company, had improperly attempted to collect personal information by insisting that he complete and return to the company an application for a program instituted by the Canada Customs and Revenue Agency (CCRA).

Summary of Investigation

The trucking company in question had sent the complainant, one of its international drivers, a letter advising that he was required to complete a "Commercial Driver Registration Application" under the new Customs Self-Assessment Program instituted by the CCRA. This letter also advised that the driver was to return the completed application to the company itself. The complainant refused, not wishing his employer to have access to the personal information he was required to provide on the application. The company sent

him a second letter ordering him to complete and return the application by a given date or else be disciplined under the collective agreement and have his employment placed in jeopardy. The complainant again did not comply, and the company terminated his employment five days after the given date. According to the company, the CCRA expected employers to gather applications and submit them to the CCRA on their drivers' behalf. In fact, the CCRA clearly instructs, on both the application form and the program pamphlet, that drivers submit their completed applications directly to the CCRA's processing centre in Niagara Falls.

Commissioner's Findings
(Issued August 17, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because interprovincial trucking companies are federal works, undertakings, or businesses as defined in the *Act*.

Application: Principle 4.4, Schedule 1, states that collection of personal information must be limited to that which is necessary for the purposes identified by the organization and that information must be collected by fair and lawful means.

The Commissioner determined that, although it was necessary for a driver to complete an application for the Customs Self-Assessment Program and return it to the CCRA, it was not necessary or appropriate for the company itself to collect the information. He also determined that threatening employees with loss of their jobs was not a fair means of collection. He found that the company was not in compliance with Principle 4.4.

The Commissioner noted that the company had been prompt in changing its policy so as no longer to require its drivers to return their applications to the company. Nevertheless, he did not consider the complaint to have been resolved, pending reinstatement of the complainant with the company and compensation for any damages. The Commissioner expressed his intention to pursue these matters with the company.

The Commissioner concluded that the complaint was well-founded.

Further Considerations

The complainant subsequently informed the Commissioner that a settlement regarding the termination of his employment had been reached through arbitration and that he considered the complaint to have thus been satisfactorily resolved.

Bank loses customer's personal information [Principle 4.7, Schedule 1, and section 12(2)]

Complaint

A customer complained that a bank had failed to protect her personal information when documents containing her Social Insurance Number (SIN), name, address and unlisted telephone number were lost during a transfer between offices.

Summary of Investigation

Human Resources Development Canada had issued the complainant a new SIN after her discovery that her old one had been used fraudulently. She later completed forms that her bank required for updating her investment account information with the new SIN. She gave the completed forms to staff at a local branch office of the bank for transfer to the office of the subsidiary that manages the investment account. The documents were lost during the transfer.

Commissioner's Findings (Issued September 7, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because banks are federal works, undertakings, or businesses as defined in the *Act*.

Application: Principle 4.7, Schedule 1, states that personal information must be protected by security safeguards appropriate to the sensitivity of the information. Section 12(2) states that the Commissioner may attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation.

At the outset of the Commissioner's investigation, the parties indicated an interest in resolving the matter. Discussions ensued, and a settlement satisfactory to both parties eventually resulted. Furthermore, the Commissioner was satisfied that the bank in question had taken steps to ensure that appropriate safeguard policies, practices, and procedures were in place.

The Commissioner concluded therefore that the complaint was resolved and no further action necessary.

Further Considerations

Both the complainant and the bank expressed satisfaction with the role that the Commissioner's Office had assumed in settling this matter.

Credit card applicant objects to bank's information-sharing policy

Complaint

An individual complained that a bank was refusing to process his credit card application because he would not consent to the bank's information-sharing policy.

Summary of Investigation

In filling out an application for a credit card, the complainant had marked up the terms and conditions by hand. His intention in doing so had been to indicate his disagreement with the bank's stated policy of sharing personal information and to exercise the option of not having his personal information shared and not receiving the bank's direct marketing service. The bank subsequently advised him by letter that it was unable to process his application as submitted because the legal wording had been amended. The complainant interpreted this letter as being a refusal on the bank's part to issue a credit card unless he authorized its information-sharing policy. In a second letter, the bank assured the complainant that applicants did have the right to opt out of the direct-marketing service and that his own application had been returned to him simply because he had altered it. The bank also offered to reconsider his credit card application and at the same time to remove his name from its direct-marketing and shared-marketing lists. The complainant agreed.

On being finally issued a credit card, the complainant pronounced himself satisfied with the bank's response and indicated that his complaint file the Office could be closed.

Accordingly, this complaint was discontinued.

Bank accused of withholding bond certificates [Principle 4.9, Schedule 1; and section 8]

Complaint

An individual complained that a bank had denied her access to her personal information in the form of two "Small Business Bonds" that she believed the bank was holding under her name.

Summary of Investigation

The complainant specified that the documents she was seeking were the paper versions or certificates of two "Small Business Bonds". In 1982, the complainant and her spouse had consolidated their outstanding indebtedness to the bank in question under the Small Business Bond (SBB) Program, a federal government initiative that provided interest relief for borrowers. The bank had advised the complainant as early as 1984 that "Small Business Bond" was only a term used and that the only actual document signed in respect of the SBB Program was a form entitled "Election in Respect of an SBB". Both the bank and Industry Canada have confirmed that this form was the only document directly related to the program; no actual paper versions or certificates of SBBs had ever existed. In 1998,

during a lawsuit over the complainant's defaulting on her loan agreement, the bank had been obliged to disclose to the complainant and her lawyer all documents it held in relation to her involvement in the SBB Program. The complainant received her signed "Election in Respect of an SBB" form at that time and was still in possession of it when she filed her complaint with the Office.

Commissioner's Findings (Issued September 18, 2001)

JURISDICTION: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because banks are federal works, undertakings, or businesses as defined in the *Act*.

APPLICATION: Principle 4.9, Schedule 1, states that upon request an individual must be informed of the existence, use, and disclosure of his or her personal information and be given access to that information. Section 8 sets out conditions under which a request may be deemed to have been refused.

The Commissioner found no evidence of the existence of SBB-related documents other than those already received by the complainant. Satisfied that the documents sought by the complainant did not exist, he found that the bank had not refused the complainant a right of access.

The Commissioner concluded therefore that the complaint was not well-founded.

Selling of information on physicians' prescribing patterns [Sections 2 and 3]

Two Complaints

In two separate complaints an individual and a physician complained that the Canadian arm of a U.S.-based international marketing firm was improperly disclosing personal information by gathering and selling data on physicians' prescribing patterns without their consent.

Summary of Investigation

The marketing firm in question gathers, from pharmacies and other Canadian sources, information related to medical prescriptions. The accumulated information includes names, identification numbers, telephone numbers, and prescribing details of physicians. This information is transferred to the firm's processing centre in the U.S., where the firm produces customized information products. These products typically identify physicians in a given territory and rank them, either individually or in groups, by monthly prescribing activity for various types or classes of drugs. The information products are then transferred to the firm's Montreal operation, where they are disclosed to clients for a fee. Pharmaceutical sales representatives from several Canadian provinces regularly buy these products.

Commissioner's Findings
(Issued September 21, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to any information disclosed outside a province for consideration. Since the information at issue was regularly transmitted across borders, the Commissioner determined that it was information disclosed outside a province for consideration and therefore that he was required to receive and investigate the complaint.

Application: Section 2 of the *Act* defines personal information as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." Section 3 of the *Act* sets out the *Act*'s purpose in terms of balancing the individual's right of privacy with the need of organizations to collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate.

The primary consideration for the Commissioner was whether the information at issue was personal information within the meaning, scope, and purpose of the *Act*. In making this determination, the Commissioner took the view that the meaning of "personal information", though broad, is not so broad as to encompass all information associated with an individual. An individual prescription, though potentially revealing about a patient, is not in any meaningful sense about the prescribing physician as an individual. Rather, it is about the professional process that led to its issuance and should be regarded as a work product – that is, the tangible result of the physician's work activity.

The Commissioner determined that interpreting "personal information" so broadly as to include prescriptions or prescribing patterns would not fulfil the purpose set out in section 3 of the *Act* (see above). Specifically, it would not be reasonable to extend the definition to prescriptions, lest it be extended also to other work products such as legal opinions or documents written in the course of employment. Nor would it be reasonable to extend the definition to prescribing patterns, lest it be extended also to patterns discoverable among other types of work products and thus preclude many kinds of legitimate commercial consumer reporting.

In sum, the Commissioner found that prescription information, whether in the form of an individual prescription or in the form of patterns discerned from many prescriptions, is not personal information about a physician.

The Commissioner concluded therefore that the complaints were not well-founded.

Further Considerations

Because of widespread public interest in the case, the Commissioner published his letter of findings as a press release, dated October 2, 2001.

F2

Estate executor disappointed in search for safety deposit box information [Principles 4.5, 4.9, Schedule 1; and section 8(7)]

Complaint

An estate executor complained that a bank had refused his request for personal information relating to the safety deposit box of his deceased aunt.

Summary of Investigation

The complainant suspected that a certain unauthorized person had, with help from the estate's lawyers, gained access to the deceased aunt's safety deposit box and removed items of value. The complainant had obtained a piece of evidence (i.e., a negative reply by fax from one branch of the bank) strongly suggesting that the bank had received at least one independent inquiry from the lawyers concerning the bank holdings of the deceased. In his capacity as estate executor, the complainant asked the bank for access to the signature card for the safety deposit box and to any correspondence between the bank and the estate's lawyers. The bank responded that it could locate neither the card nor any such correspondence. An exhaustive search of the bank files, involving the bank's own ombudsman, the Canadian Banking Ombudsman, and the Office of the Privacy Commissioner, proved unsuccessful in locating any of the information sought by the complainant.

Normally, the bank keeps safety deposit box signature cards for seven years. All the safety deposit boxes had been transferred from one branch of the bank to another eight days after the aunt's death, but appropriate security measures had been taken during the transfer. It was not bank policy for a branch to keep records of an account, an investment, or a safety deposit box once transferred to another branch. Nor was it bank policy for a branch to keep requests for information pertaining to a file it no longer held.

Commissioner's Findings (Issued October 12, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because banks are federal works, undertakings, or businesses as defined in the *Act*.

Application: Principle 4.9, Schedule 1, states that upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. Section 8(7) states that an organization that responds within the time limit and refuses a request shall inform the individual in writing of the refusal, setting out the reasons and any recourse that they may have under this part.

The Commissioner determined that the information the bank could not produce should have been retained in accordance with Principle 4.5 or should not have been lost.

He therefore found that the bank had not complied with Principle 4.9. He also found that the bank's response constituted a refusal under section 8(7).

The Commissioner concluded therefore that the complaint was well-founded.

Further Considerations

The Commissioner recommended that the bank revise its practices concerning the destruction of documents containing personal information and develop a written policy on the retention of such documents in conformance with the relevant provisions of the *Act*.

Employee alleges non-consensual disclosure by employer to investment firm [Section 7(3) and Principles 4.3 and 4.5, Schedule 1]

Complaint

An employee of a large corporation complained that his employer was improperly disclosing his and other employees' personal information, including information related to cash bonuses, without the employees' consent or prior knowledge, to the investment firm involved in an RRSP and savings plan sponsored by the corporation.

Summary of Investigation

The corporation in question has admitted that it discloses employees' personal information without their explicit consent to the investment firm involved in its RRSP and savings plan for hourly employees. The information disclosed consists of the individual's payroll and personal identification numbers, name, address, social insurance number, marital status, gender, preferred language, seniority service date, birth date, department, group code, and union code. The corporation also informs the investment firm when it awards cash bonuses, but does not specify the recipient or the amount of the bonus. The RRSP and savings plan was established by the corporation in fulfillment of a commitment under its collective agreement with the employees' union. The corporation pays the investment firm for the services it provides under the plan and does not disclose the information to the investment firm for consideration, monetary or otherwise.

Commissioner's Findings (Issued October 18, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies strictly to federal works, undertakings, or businesses or to disclosures of personal information across borders for consideration. The corporation in question is neither a federal work, undertaking, or business as defined in the *Act*, nor does it disclose the personal information at issue across borders for consideration.

The Commissioner concluded that he lacked jurisdiction to pursue the matter further.

Requester alleges non-receipt of credit report from agency [Section 8]

Complaint

An individual complained that a credit-reporting agency refused his request to disclose his credit report to him.

Summary of Investigation

The complainant had written to the credit reporting agency to request access to any credit report the agency held on him. In his complaint, he alleged that he did not subsequently receive a response from the agency. The agency's consumer relations centre has a staff of six who are responsible for receiving and processing access requests according to standard procedures. By those procedures, a client request is not filed unless it has been matched to a credit report that has either been mailed or handed to the client. The centre does have on file a copy of the complainant's access request, with a handwritten notation to the effect that a response was mailed to the complainant's correct address 13 days after receipt of the request. The mailing of a response was also confirmed by reference to a computerized log and a computer-generated audit report. The complainant at one point allowed the possibility of having merely overlooked the credit report on receiving it. Later he declared it highly unlikely that he had received the report without noticing it.

Commissioner's Findings (Issued October 26, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to disclosures of personal information across borders for consideration. The Commissioner had jurisdiction in this case because the credit reporting agency in question had disclosed personal information across borders for consideration.

Application: section 8(3) of the *Act* states that an organization shall respond to a request with due diligence and in any case not later than 30 days after receipt of the request. Section 8(5) states that if the organization fails to respond within the time limit, the organization is deemed to have refused the request.

The Commissioner found no reason to doubt the evidence that the credit-reporting agency had received the complainant's access request and mailed a response within the time limit prescribed. He found that the agency had complied with section 8(3) of the *Act*.

The Commissioner concluded that the complaint under section 8(5) was not well-founded.

Airline accused of refusing access to personal information about vacation incidents [Principles 4.1 and 4.9, Schedule 1]

Complaint

Three air travellers complained that an airline company had denied them access to personal information about their experiences during a Mexican vacation.

Summary of Investigation

The complainants had requested access to all personal information the airline and its travel affiliate held regarding certain incidents they had experienced during a vacation in Mexico. A representative responded initially that the company was under no obligation to provide such information. On being advised of its obligations under the *Personal Information Protection and Electronic Documents Act* by the Office of the Privacy Commissioner, the company took immediate action to appoint an official to be accountable for compliance with the *Act*, processed the complainants' access request, and sent them the personal information requested. On reviewing this information, the complainants were of the opinion that the company had not included incident reports. The investigator for the Privacy Commissioner examined the company's original files containing the complainants' personal information, but found no evidence of information other than that which the complainants had already received. The company confirmed in writing that it did not have in its possession any additional information about the complainants, including incident reports.

Commissioner's Findings (Issued October 31, 2001)

Jurisdiction: As of January 1, 2001, the *PIPED Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because airlines are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Principle 4.1, Schedule 1, states that an organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with [the principles in] Schedule 1. Principle 4.9 states that upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information.

Regarding Principle 4.1, the Commissioner determined that the airline company had not designated an individual until his Office intervened. He found therefore that the company had initially failed to comply with this principle. However, he also noted that the company had subsequently designated a senior official responsible for ensuring compliance with the *Act*. The Commissioner considered this issue resolved.

Regarding Principle 4.9, the Commissioner likewise determined that the company had provided the complainants with their personal information only after intervention by his Office. He found therefore that the company had not initially been in compliance with this principle. He noted, however, that the complainants were satisfied that they had received all of their personal information in the company's possession; they were also satisfied with the outcome of the investigation.

The Commissioner concluded that the complaint was well-founded and resolved.

Employee objects to employer's use of bank account number on pay statement [Principles 4.3 and 4.7, Schedule 1]

Complaint

An employee of a telecommunications company complained that her employer:

1. Used her personal information for a purpose without her consent by printing her bank account and bank transit numbers on her pay statements; and
2. Did not adequately safeguard employees' pay statements given the sensitivity of the information in them.

Summary of Investigation

The employees of the telecommunications company in question receive their pay by direct deposit and their pay statements by delivery in sealed envelopes at the workplace. As a result of a merger and a subsequent conversion of payroll systems, bank account and bank transit numbers began to be included on all employees' pay statements as of January 1, 2001. Printing of such numbers on pay statements has become standard practice in both the private and the public sectors. On this company's statements, there is no indication what the numbers refer to; only a person familiar with the bank's information codes would know what the numbers represent. On delivery to the complainant's workplace, the sealed envelopes containing employees' pay statements are collected together in a larger envelope and left on a manager's desk, where they often remain unsecured and largely unattended for periods as long as 24 hours.

The complainant had originally consented to having her pay deposited directly into her bank account, but had never explicitly consented to having the numbers appear on her statement. She believed that her employer was thus using her personal bank account information without her consent and for a purpose inconsistent with that for which she originally had provided it. She also believed that her employer did not adequately safeguard employee pay statements at her workplace.

The company's position was that the information was still being used only for the original purpose of directly depositing payroll funds; that the practice of printing account and

branch numbers on pay statements had become imperative for purposes of verifying allocations of funds and resolving discrepancies; and that many employees had already come to expect and rely upon the appearance of these numbers on their statements. The company also argued that it did adequately safeguard its employees' bank account information by delivering statements in confidential sealed envelopes.

Commissioner's Findings (Issued November 5, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because telecommunications companies are federal works, undertakings, or businesses as defined in the *Act*.

Application: Principle 4.3, Schedule 1, states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. This principle also stipulates (4.3.5) that the reasonable expectations of the individual are relevant. Principle 4.7 states that personal information shall be protected by appropriate security safeguards appropriate to the sensitivity of the information.

On the first aspect of the complaint (consent), the Commissioner determined that employees who provide their bank account and bank transit numbers for direct-deposit purposes could reasonably expect those numbers to appear on transaction records for the entirely consistent purpose of verifying proper allocation of funds. He was satisfied that the complainant had thus implicitly given consent. He found that the company therefore had met its obligations under Principle 4.3, Schedule 1.

The Commissioner concluded that this aspect of the complaint was not well-founded.

On the second aspect of the complaint (security safeguards), the Commissioner determined that the company's operational controls at the complainant's workplace were not consistent with the sensitivity of the personal information contained in the pay statements. He found that the company did fail to meet its obligations under Principle 4.7, Schedule 1.

However, he noted that the company, on being informed of its obligations, had taken immediate and appropriate steps to correct its information management practices related to employee pay statements.

The Commissioner concluded that this aspect of the complaint was well-founded and resolved.

Further Considerations

As a short-term solution, the company agreed to implement tighter operational controls at the complainant's own workplace and offered the complainant the option of having her pay statement mailed to her home.

Company asks for customer's SIN as matter of policy [Principles 4.3.3 and 4.4.1, Schedule 1; and section 5(3)]

Complaint

An individual complained that a telecommunications company had improperly collected her personal information in the form of her Social Insurance Number (SIN).

Summary of Investigation

In signing-up the complainant for Internet connection, the telecommunications company in question had asked her for her SIN. According to the complainant, the company representative with whom she had spoken had told her, "No SIN, no connection," and she had therefore felt obliged to give up her number in order to obtain the service. It was the company's written policy to collect SINs from persons requesting services. The purpose of this policy was to avoid confusion over similar names among customers. However, by the same policy, the company did not insist on obtaining the SIN in cases where the customer refused and did advise its employees that the collection was not obligatory.

Commissioner's Findings (Issued November 5, 2001)

JURISDICTION: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because telecommunications companies are federal works, undertakings, or businesses, as defined in the *Act*.

APPLICATION: Principle 4.3.3, Schedule 1, states that an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes. Principle 4.4.1 states that organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Section 5(3) states that an organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

Regarding Principle 4.4.1, the Commissioner determined that, by the company's own policy, the collection of SINs was non-obligatory and therefore not necessary to fulfil explicitly specified and legitimate purposes. He found that the collection was thus indiscriminate and that the company was not in compliance with this principle.

Regarding Principle 4.3.3, the Commissioner was satisfied that the complainant had clearly received the impression that giving her SIN was a condition of service. He found therefore that the company was not in compliance with this principle.

Regarding section 5(3), the Commissioner was mindful of his Office's longstanding position that the SIN should not be used as a universal identifier and that citizens should not give out their SINs unless legally required to do so for purposes of the limited number of federal government programs authorized for such collection. He was satisfied that a reasonable person would object to the collection of SINs for purposes of Internet connection. He found that the company was therefore not in compliance with section 5(3).

The Commissioner noted that the company had removed the SIN from the complainant's file and was in the process of changing its policy so that SINs would no longer be requested.

The Commissioner concluded therefore that the complaint was well-founded and resolved.

Further Considerations

The Commissioner also recommended that the company take steps to review its files and remove any other unnecessary SINs collected from its other customers.

User accuses ISP owner of reading and blocking her e-mail [Principle 4.3, Schedule 1]

Complaint

An individual complained that the owner of her former Internet service provider (ISP):

1. Had improperly collected her personal information without her consent in that he had read her e-mails; and
2. Was blocking e-mail she was attempting to send through a new ISP to users of her former ISP.

Summary of Investigation

The complainant had been a subscriber with a certain ISP for two years. During that time, she had had a disagreement with the ISP owner concerning her use of her account, specifically her attempts to transmit large files by e-mail. She alleged that during that disagreement the owner had told her that he could read her e-mails. She further alleged that, after she had moved to another city and subscribed with a different ISP, the same owner had begun to block the e-mails she was trying to send to users of her former ISP.

The owner in question said that he could not remember any disagreement with the complainant, but he did allow that, on detecting a large number of "delivery failure" messages (indicating attempts to transmit large files by e-mail), it would have been his usual practice to call the user and discuss the matter. He denied being able to read anything other than "delivery failure" messages in relation to the complainant's account. He also denied blocking her messages.

The investigation confirmed that the ISP in question can monitor users' account activity and detect "delivery failure" messages, but does not receive e-mails or attachments and cannot read the content of users' e-mail messages. Nor was there any evidence that the owner had been blocking the complainant's

e-mails from her new server. In fact, several weeks before the owner was notified of the complaint against him, the blocking problem ceased when a computer technician changed the Internet protocol address on the complainant's computer.

Commissioner's Findings (Issued November 5, 2001)

JURISDICTION: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because Internet service providers are federal works, undertakings, or businesses as defined in the *Act*.

APPLICATION: Principle 4.3, Schedule 1, states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

The Commissioner was satisfied that the ISP could not read its users' e-mails and had not blocked the complainant's messages. He also determined that a reasonable person would expect the ISP to monitor the services it provides and respond to persistent "delivery failure" messages. He found that the ISP in this case was not in contravention of Principle 4.3, Schedule 1.

The Commissioner concluded therefore that the complaint was not well-founded.

Employer sends third parties copies of response to employee's access requests [Principles 4.3 and 4.5, Schedule 1; and section 5(3)]

Complaint

An employee of an airport authority complained that her employer had, without her consent, disclosed to three third parties her personal information in the form of copies of a letter of response to access requests she had made.

Summary of Investigation

The complainant had submitted requests under the *Personal Information Protection and Electronic Documents Act* for access to information held by her employer. The employer subsequently sent her a letter of response to the effect that the organization was refusing her requests. This letter also indicated that copies were being sent to three other persons – specifically, two union representatives and the coordinator of employee relations at the airport. The complainant had not sent copies of her access requests to these parties and had not explicitly consented to having copies of the response letter sent to them.

The union representatives had previously attended the meeting at which the issue of access to the complainant's personal information had first been raised. The employee relations coordinator had previously intervened in a harassment complaint filed by the same complainant and had in his possession certain

related documents to which the complainant had requested access. On the grounds of these prior involvements, the employer argued that the complainant had implicitly consented to the disclosures. The complainant maintained that she had submitted the access requests personally on her own behalf, without union intervention.

Commissioner's Findings (Issued November 5, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because airports are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Principle 4.3, Schedule 1, states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. Principle 4.5 states that personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Section 5(3) states that an organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

Regarding Principle 4.3 and the disclosure to the union representatives, the Commissioner determined that there would have been implied consent for the employer to send response copies to those parties only if the complainant had indicated that she had sent them copies of her access requests. The complainant had the right to exercise her formal recourse without union intervention, and it was not necessary for the employer to inform the union of its response. The Commissioner found that no implied consent had existed as far as the union representatives were concerned. Furthermore, in consideration of section 5(3), he was satisfied that a reasonable person would have considered the disclosure to the union representatives to be unacceptable.

He concluded therefore that this aspect of the complaint was well-founded.

Regarding Principle 4.5 and the employee relations coordinator, given the direct involvement of that party in the access request, the Commissioner determined that it had been appropriate for the employer to inform him of its decision to refuse the complainant access to the documents she had requested. Furthermore, in consideration of section 5(3), the Commissioner was satisfied that a reasonable person would have considered the communication to the employee relations coordinator to be acceptable. He found that the employer was thus in compliance with Principle 4.5 as far as the employee relations coordinator was concerned.

He concluded therefore that this aspect of the complaint was not well-founded.

Further Considerations

During the investigation, the Office of the Privacy Commissioner advised the airport authority in question that it is prefe.able not to send copies of responses to third parties, but rather to allow the individual requester to judge whether or not to share a response with others after receiving it. The Commissioner was pleased to note that the organization had followed this advice in dealing with subsequent access requests by the complainant.

Telephone company demands identification from new subscribers [Principles 4.2, 4.2.3 and 4.3, 4.3.2, 4.3.3 Schedule1; and section 5(3)]

Complaint

An individual complained that a telecommunications company's collection of personal information from new subscribers was inappropriate, in that the company required a deposit from new customers who refused to supply the information.

Summary of Investigation

When the complainant attempted to obtain a new telephone service from the company in question, an operator asked her to supply two pieces of personal identification. When the complainant expressed reluctance, the operator told her that she would have to provide a deposit if she did not comply. The operator also told her that the purpose of the information collection was to confirm her identity. A company supervisor subsequently gave her the same explanation for the collection and confirmed that she would have to provide a deposit if she did not supply the information.

It is company policy for operators to ask new subscribers for two pieces of identification, to demand a deposit in cases of refusal, and to explain the information collection simply as confirmation of identity. However, in cases where an applicant is a new customer with no previous business relationship with the company, the actual purpose of the collection is to run a credit check on the applicant, in accordance with CRTC regulations, given that the provision of telephone services constitutes an extension of credit on the company's part.

Commissioner's Findings (Issued November 8, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because telecommunications companies are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Principle 4.2.3 states that purposes should be identified at or before the time of collection. Principle 4.3.2 states that organizations must make a reasonable effort to advise the individual concerned of the purposes for which the information will be used and must do so in such manner that the individual can reasonably understand.

Principle 4.3.3 states that organizations must not, as a condition of supplying a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes. Section 5(3) states that an organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

Regarding Principle 4.3.3 and section 5(3), the Commissioner determined that a reasonable person would consider it appropriate for the company to collect personal information for the purpose of confirming whether a potential customer is credit worthy or, in the case of repeat customers, confirming identity.

He concluded that this aspect of the complaint was not well-founded.

Regarding Principles 4.2.3 and 4.3.2, the Commissioner determined that a reasonable person would conclude that the company did not explicitly state the purpose for its collection of personal information with respect to first-time subscribers.

He concluded that this aspect of the complaint was well-founded.

Further Considerations

The company agreed to amend its practice in identifying purposes. Specifically, the company will inform first-time subscribers that the purpose of its information collection is to assess credit-worthiness given that the company supplies credit in the form of long-distance calling service.

Broadcaster accused of collecting personal information via Web site [Section 2; and Principle 4.3, Schedule 1]

Complaint

An individual complained that a broadcaster had attempted, through its advertising server, to collect his personal information, specifically the NETBIOS information on his computer, without his consent.

Summary of Investigation

The complainant had a computer equipped with both a cable modem for Internet connection and a firewall designed to detect and block attempts at intrusion. Every time he tried to log onto the organization's Web site, his firewall detected, rejected, and reported on, an attempt by the broadcaster's advertising server to gain access to the NETBIOS information on his computer. A NETBIOS is a computer's common or "friendly" name related to its Internet protocol (IP) address. If an IP address is traced, it allows access to information such as Web sites visited by the computer's user or recent passwords used in obtaining access to secure accounts. The likelihood of tracing an IP address is small if the user has dial-up Internet access, but significantly greater if the user has a fixed Internet connection via a cable modem, as was the case with the complainant.

After conducting internal inquiries, the organization confirmed that the complainant's allegation was true. The broadcaster explained that the network administrator, on installing Microsoft Windows NT, had neglected to deactivate certain features that come automatically with that program. These features, known as Internet Name Services, enable a server to collect the NETBIOS information of Web site users. Once informed that the features were on, the network administrator promptly turned them off. The complainant subsequently confirmed that his firewall no longer detected any attempts by the organization to obtain his NETBIOS information.

Commissioner's Findings (Issued November 20, 2001)

JURISDICTION: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings or businesses. The Commissioner had jurisdiction in this case because broadcasters are federal works, undertakings or businesses, as defined in the *Act*.

APPLICATION: section 2 of the *Act* defines personal information to be "… information about an identifiable individual …". Principle 4.3 of Schedule 1 states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

The Commissioner was satisfied that in some circumstances, notably the complainant's, a NETBIOS might be used to obtain information traceable to an identifiable individual. He determined therefore that the information at issue was personal information for purposes of the *Act*.

The Commissioner found that the broadcaster had failed to meet its obligations under Principle 4.3. However, he did not dispute the broadcaster's explanation that this failure had been unintentional, and he noted that its response had been satisfactory.

He concluded therefore that the complaint was well-founded and resolved.

Couple alleges bank withheld loan information [Sections 8(3) and 8(5)]

Two Complaints

A husband and wife complained in two separate complaints that a bank had denied them access to their personal information in that it had not responded to their request for information related to a loan application.

Summary of Investigation

The complainants had written, jointly signed, and submitted two letters requesting personal information about two different credit products from their local branch of the bank in question. The letters were identical, except for their subject lines, one of which referred to a numbered loan application and the other to a

numbered mortgage, both relating to the complainants. Within the month, the bank sent them the information they had requested about their mortgage, but no information about their loan application. The complainants wrote the bank another letter, outlining in greater detail the information they were seeking about the loan application. Approximately one month after this second submission, a lawyer for the bank responded, informing the complainants only that they would be required to pay photocopying charges of 25 cents per page. The complainants then submitted another letter in which they enclosed a cheque to cover reproduction costs and confirmed that they still wanted the information in question. When they received no further response after three weeks, they filed their complaints with the Office of the Privacy Commissioner.

The bank at first denied the allegation, insisting that the complainants' second submission had been the first to make reference to the loan application. However, on being presented with a copy of the letter containing the prior reference, the bank checked its records and acknowledged receipt of that earlier letter. The bank explained that its failure to respond had been unintentional, in that the employee who had received the first submission had not noticed the different subject headings on the two similar-looking letters, had assumed they were identical, and had therefore forwarded only one of them (the one referring to the mortgage) on for response.

Commissioner's Findings (Issued November 26, 2001)

Jurisdiction: As of January 1, 2001, the *Personal Information Protection and Electronic Documents Act* applies to federal works, undertakings, or businesses. The Commissioner had jurisdiction in this case because banks are federal works, undertakings, or businesses, as defined in the *Act*.

Application: Section 8(3) of the *Act* states that an organization shall respond to a request with due diligence and in any case not later than thirty days after receipt of the request. Section 8(5) states that if the organization fails to respond within the time limit, the organization is deemed to have refused the request.

The Commissioner found that the bank had failed to respond within the time limit and was thus in contravention of section 8. However, he was satisfied that this failure had been unintentional, and he noted that the bank had subsequently provided to the complainants all the information they had sought.

He concluded therefore that the complaints were well-founded and resolved.

Incidents under *PIPED Act*

Incidents are matters that come to my attention through various sources including issues raised in the media. These are usually issues where there is no identified victim and where no complaint has been filed. During the past 11 months my Office has looked into the following two incidents.

Transportation company collects, discloses passengers' personal information

Incident

It was alleged that a transportation company's sales agents were:

1. asking for date of birth and citizenship as well as name from individuals making train bookings by phone or in person for the Toronto-to-New York run; and
2. disclosing this information to United States Customs (USC) and the United States Naturalization and Immigration Service (USNIS).

Summary of Investigation

The Canadian company confirmed that the practice in question has been taking place since December 2000, by agreement among the company, the U.S. transportation company, Canada Customs and Revenue Agency, and USC/USNIS. The purpose is to minimize delays at the Canada/U.S. border. The personal information thus collected is stored in the company's reservation computer system and deleted if the individual does not eventually purchase the ticket. If the passenger does purchase the ticket, his or her name, date of birth, and citizenship are printed on a manifest, which is then faxed to USC/USNIS and a copy given to the service manager on board the train. The service manager destroys the manifest shortly after the trip is completed.

The Office of the Privacy Commissioner of Canada determined that the sales agents, on written instruction from the company, had been representing the practice as a requirement for passengers on the Toronto-to-New York run.

Outcome

The company asked the Office of the Privacy Commissioner of Canada for instructions on an acceptable resolution to the problem. The Office advised that it issue to its sales agents a clear directive to the effect that passengers' provision of date of birth and citizenship must be represented as voluntary and that agents may, after booking a ticket, ask customers whether they would be willing to provide this information in order to facilitate customs clearance at the border.

On receiving a copy of such a directive sent by the company to its sales agents, the Office informed the company that the incident file would be closed, subject to the Office's continued monitoring of sales agents' booking practices. The Office also advised that at some point the company send its sales agents a follow-up note clarifying in stronger terms that they are not to collect personal information at the time of booking without the informed consent of the individual.

Web site broadcasts cell phone conversations

Incident

The *Ottawa Sun* reported on June 7, 2001, that an Ottawa-based Web site was streaming live audio from cellular telephones onto the Internet from a radio.

A scanner was intercepting cellular telephone traffic. The scanner was connected to a computer that was hosting a Web site. By connecting to the Web site, anyone could listen in on private cell phone conversations.

Outcome

As the Office of the Privacy Commissioner began its investigation, the Internet service provider (ISP) in question shut down the Web site because of bandwidth problems. This was caused by an employee who had a personal network account that had been forwarding data through another server. On discovery, the ISP had immediately relieved the employee of his duties. The ISP indicated that the Web site in question had moved to a New York server under new management.

Given that the Ottawa-based Web site had been shut down, the Office's investigation was discontinued. The Web site will be monitored periodically for an indefinite length of time.

Inquiries by type under *PIPED Act*
January 1, 2001 to November 30, 2001

Subject	Number
Criminal records	30
Drug Testing	3
Encryption	7
Financial Institutions	1,519
Identity Theft	38
Information Request	2,558
Interception/monitoring	154
Interpretation	2,024
Jurisdiction	1,975
Marketing	439
Medical Records	137
Calls from Members of Parliament	7
Publication Requests	675
Social Insurance Number	1,834
Telecommunications	786
Transportation	139
Other	388
Total	12,713

Privacy Practices and Reviews

The *Personal Information Protection and Electronic Documents Act* allows me to audit the compliance of private organizations if I have "reasonable grounds to believe" that the organizations are contravening a provision of the *Act*.

Following accepted standard audit objectives and criteria, the Privacy Practices and Reviews Branch of my Office will conduct compliance reviews and audits under section 18 of the *Act*. As it has come into effect at the beginning of this year, I have not yet initiated any such audit. I have focused instead on educating businesses and organizations on the impact of the new legislation, and giving them guidance for establishing privacy policies that comply with it.

In the Courts

Mathew Englander v. Telus Communications Inc.

This is the first application for judicial review to be filed in the Federal Court under the *PIPED Act*. Mathew Englander filed a complaint with the Office of the Privacy Commissioner on January 1, 2001 claiming, *inter alia*, that Telus uses and discloses customers' names, addresses and telephone numbers in its White Pages directories and otherwise, without customers' knowledge and consent and that Telus inappropriately charges customers for choosing to have their telephone number "non-published". The applicant submitted that these actions by Telus contravene subsections 5(1) and (3) of the *PIPED Act* as well as several clauses of Schedule 1 of the *PIPED Act*.

After investigating the complaint, I concluded that Telus is in full compliance with the *Act* in respect of the matters of which the complaint was made. I concluded that a reasonable person would consider Telus' initiation of service practice and subsequent publishing of customers' personal information in its white pages is an appropriate collection, use and disclosure of the information. I further concluded that Telus has the authority to charge its customers a fee for non-published telephone

service and that this is not an unreasonable practice so as to contravene principle 4.3.3 of Schedule 1.

I found the complaint not well-founded. As permitted by section 14 of the *PIPED Act*, Mr. Englander has applied to the court for a hearing in respect of the matter.

Ronald G. Maheu v. The Attorney General of Canada and IMS Health Canada

The applicant has applied for a hearing in the Federal Court, as permitted under section 14 of the *PIPED Act*, after having complained to me that IMS Health improperly discloses personal information by gathering and selling data on physicians' prescribing patterns without their consent.

After having investigated the matter, I found that prescription information, whether in the form of an individual prescription or in the form of patterns discerned from many prescriptions, is not personal information about a physician. In determining whether the information at issue was personal information within the meaning, scope and purpose of the *Act*, I took the view that the meaning of "personal information", though broad, is not so broad as to encompass all information associated with an individual. I found that an individual prescription, though potentially revealing about a patient, is not in any meaningful sense about the prescribing physician as an individual but is about the professional process that led to its issuance and should be regarded as a work product – that is, the tangible result of the physician's work activity. In sum, I concluded that the complaint was not well-founded.

Mr. Maheu has applied to the court for a hearing in respect of this matter. Included in the Notice of Application was a request by the applicant, under the Federal Court rules, that my Office transmit material in its possession to the applicant and the Registry of the Federal Court. The Office of the Privacy Commissioner has objected to the request, as all documents not already in the possession of the applicant cannot be disclosed by the Privacy Commissioner pursuant to provisions of the *PIPED Act*.

Communications and Public education

Under the *PIPED Act*, my Office was given a broader mandate for public education in order to increase awareness and understanding of privacy issues. To focus on this important new responsibility, establishing the Communications and Strategic Analysis Branch was one of the first steps I took following my appointment. This branch has undertaken a number of activities during the past year to help raise awareness of privacy issues and to inform Canadian citizens and businesses about the new private sector legislation.

Public speaking is an invaluable tool that helps me fulfill my responsibility for promotion, public education and awareness of privacy issues. I have given 35 speeches to a range of organizations across Canada and internationally over the past year. Another 31 speeches were delivered by other senior staff. Speeches have focused on the major issues of the day, such as the security versus privacy debate that ensued following the Sept. 11 attacks on the U.S. Many other speaking engagements have been used to tell citizens and businesses alike about the new *Act* and how it affects them, to discuss privacy in the workplace, and to raise privacy concerns about specific initiatives, including Government On-Line, electronic health records and the growing use of video surveillance.

As well, recognizing the influence of the media in setting the agenda for public debate and in raising public awareness, my Office has begun to proactively track privacy issues in the media and has become much more engaged in a variety of media relations activities.

These activities have included disseminating public statements, news releases and feature articles to both mainstream and targeted media; granting media interviews and participating in editorial board meetings; and providing media relations support for speeches, conferences and other special events. In addition, my Office has responded to inquiries from the media, providing comment and background information on a wide variety of privacy-related issues.

Every month, the number of media queries continues to increase, currently averaging anywhere from 80 to 100 per month. In addition, I have granted more than 210 media interviews since September 2000.

Public education materials

My Office has produced and distributed promotional and educational material to satisfy an increased demand for information under the *PIPED Act*. We have published comprehensive guides to the new *Act* for both businesses and individuals. More than 21,000 of both of these guides have been distributed during 2001.

In addition, we have created posters, privacy kits, notepads and bookmarks. All these products help to satisfy the demand for more information on privacy issues by individuals, businesses and other organizations.

Advertising

As part of the public outreach program to raise awareness of the new privacy rights of Canadians in the private sector, beginning with federally regulated businesses, my Office placed advertisements in more than 1,300 daily and community newspapers in all parts of Canada, These ads were directed at informing Canadians of their rights under the *PIPED Act*. The advertisement, under the banner "Your privacy is our concern" and « Votre vie privée, ça nous regarde », which ran in March 2001, reached millions of Canadians in all regions of the country.

A second advertisement ran in the 12 newspapers in the three territories, pointing out that the *Personal Information Protection and Electronic Documents Act* applies to all businesses in the territories as they are considered to be federal works and undertakings. Following the appearance of the advertisements, my Office noted a significant increase in the number of inquiries and requests for further information about the *PIPED Act*.

Web Site

Over the past year, my Office's Web site has undergone a complete redesign and considerable expansion as part of our greater mandate for public education and awareness under the new *Act*.

Every effort is made to ensure the Web site is an up-to-date resource for privacy information, as well as a useful tool for research on privacy-related issues. Ultimately, the redesigned Web site is more interactive, user-friendly and relevant to both individuals and businesses.

I am pleased to report that the Web site is an increasingly efficient tool for reaching Canadians and others with information about privacy issues. Visits to our site continue to increase, with an average of 11,500 visits per month.

Communications Activities

January 1, 2001 to November 30, 2001

Activity		Number
Speeches delivered by Privacy Commissioner		35
Speeches delivered by senior staff		31
News Releases		15
Media Interviews		210
Distribution of materials		**27,586**
Business Guides	13,005	
Citizen's Guides	8,707	
Other (Annual Reports, bookmarks, fact sheets, *Acts*, etc.)	5,874	
Average number of visits to Web site per month		11,500

Part Three Corporate Services

Gearing up for implementation of the Private Sector Act

The Office has increased the size of its staff and budget to prepare for implementation of the *Personal Information Protection and Electronic Documents Act,* which started coming into effect January 1, 2001.

Our budget was increased to more than $11 million per year beginning April 1, 2001, up from $8.7 million for 2000-2001. This budget increase enabled my Office to make a number of important changes, which included:

- increasing inquiries staff to handle an increase in the number of calls;
- extending our hours from 9 a.m. to 5 p.m. in all time zones across Canada;
- establishing the Privacy Practices and Reviews Branch to handle audits under the *Personal Information Protection and Electronic Documents Act* and to continue work in the public sector;
- establishing a Communications and Strategic Analysis Branch, incorporating the existing research function, to focus on communications and public education, and to ensure that we are a centre of expertise on issues related to privacy; and
- increasing the number of investigators to handle complaints under both *Acts.*

A long-term financial framework for future funding will be presented to the Treasury Board of Canada Secretariat in 2003-2004.

Resources

(April 1, 2000 to March 31, 2001)

	FTEs	Expenditure Totals	Percentage of Total
Privacy	56	$ 7,418,451	89%
Corporate Services	10	$ 941,369	11%
Total	**66**	**$ 8,359,820**	**100%**

Note: FTE stands for "full-time equivalent" or full-time staff.

Detailed Expenditures[1]
April 1, 2000 to March 31, 2001

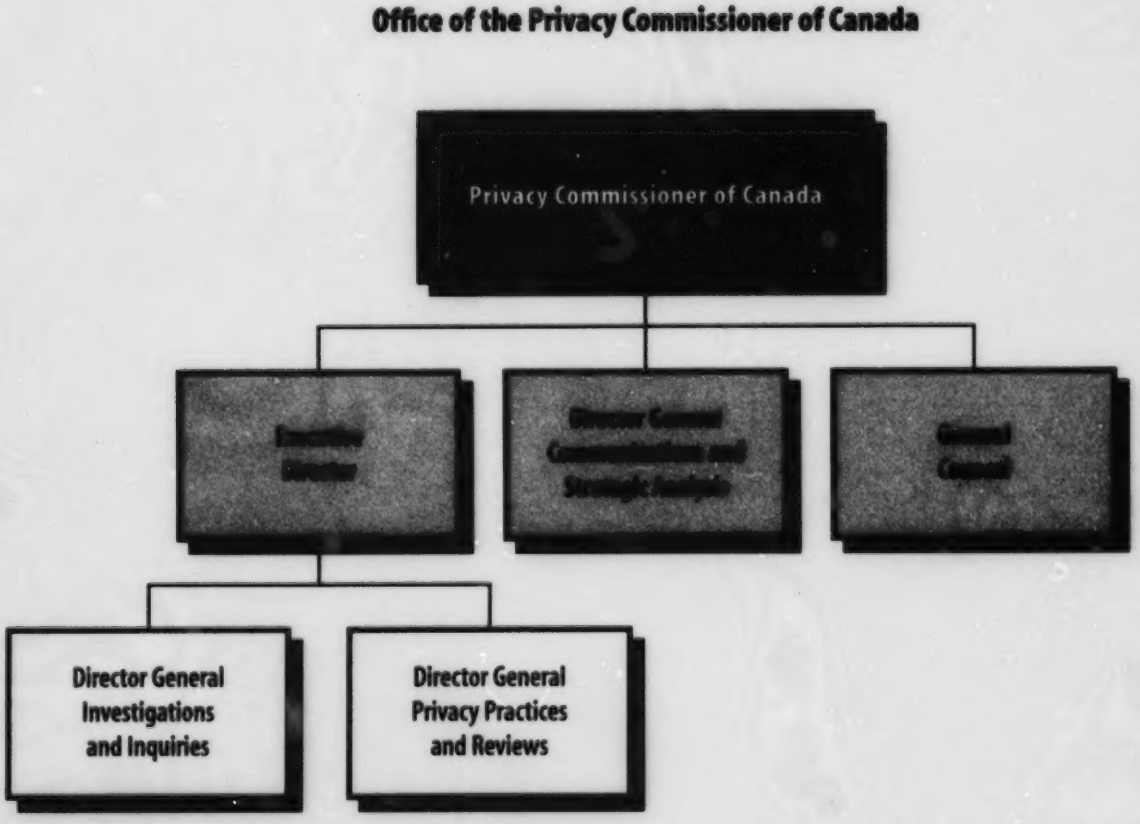
	Privacy	Corporate Services[2]	Total
Salaries	$3,776,280	$464,091	$4,240,371
Employee Benefit Plan Contributions	611,000	84,500	695,500
Transportation and Communication	268,588	93,470	362,058
Information	979,136	1,993	981,129
Professional Services	600,427	121,197	721,624
Rentals	33,036	13,958	46,994
Repairs and Maintenance	327,711	32,721	360,432
Materials and Supplies	62,616	28,400	91,016
Acquisition of Machinery and Equipment	759,403	100,998	860,401
Other Subsidies and Payments	254	41	295
Total	$7,418,451	$941,369	$8,359,820

Notes:

[1] Expenditure figures do not incorporate final year-end adjustments.

[2] Expenditures for Corporate Services are allocated on a 50/50 basis and shared between the Offices of the Privacy Commissioner of Canada and the Information Commissioner of Canada.

Corporate Structure



Commissaire à la protection de la vie privée du Canada

The Privacy Commissioner of Canada

Rapport annuel au Parlement 2000-2001

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

(613) 995-8210, 1-800-282-1376
Téléc. (613) 947-6850
ATS (613) 992-9190

© Ministre des Travaux publics et Services gouvernementaux Canada 2001
N° de cat. IP30-1/2001
ISBN 0-662-66226-1

Cette publication est également disponible sur notre site Web à www.privcom.gc.ca

Office of the Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissariat à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Télec.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Décembre 2001

L'honorable Daniel Hays
Président
Sénat du Canada

Monsieur,

J'ai l'honneur de remettre au Parlement mon rapport annuel pour les périodes du 1er avril 2000 au 31 mars 2001 dans le cas de la *Loi sur la protection des renseignements personnels* et du 1er janvier 2001 au 30 novembre 2001 dans le cas de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Le moment de la parution du rapport de cette année est exceptionnel. J'avais décidé de remettre mon rapport au début de l'automne cette année plutôt qu'au printemps comme d'habitude, pour deux raisons : tout d'abord, étant entré en fonction en septembre 2000, je voulais une période suffisante d'expérience sur laquelle fonder mon rapport; et, en second lieu, vu que la *Loi sur la protection des renseignements personnels et les documents électroniques* est entrée en vigueur le 1er janvier 2001, je préférais que le rapport fasse état d'une expérience suffisante de la nouvelle loi. Puis, les événements du 11 septembre, et les questions de protection des renseignements personnels qu'ils ont soulevées, m'ont obligé à attendre jusqu'à maintenant. Le Commissariat reviendra à son échéancier normal avec un rapport le printemps prochain.

Veuillez agréer, Monsieur, l'expression de mes sentiments les meilleurs.

Le Commissaire à la protection
de la vie privée du Canada,

George Radwanski

Office of the Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissariat à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Téléc.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Décembre 2001

L'honorable Peter Milliken
Président
Chambre des communes

Monsieur,

J'ai l'honneur de remettre au Parlement mon rapport annuel pour les périodes du 1er avril 2000 au 31 mars 2001 dans le cas de la *Loi sur la protection des renseignements personnels* et du 1er janvier 2001 au 30 novembre 2001 dans le cas de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Le moment de la parution du rapport de cette année est exceptionnel. J'avais décidé de remettre mon rapport au début de l'automne cette année plutôt qu'au printemps comme d'habitude, pour deux raisons : tout d'abord, étant entré en fonction en septembre 2000, je voulais une période suffisante d'expérience sur laquelle fonder mon rapport; et, en second lieu, vu que la *Loi sur la protection des renseignements personnels et les documents électroniques* est entrée en vigueur le 1er janvier 2001, je préférais que le rapport fasse état d'une expérience suffisante de la nouvelle loi. Puis, les événements du 11 septembre, et les questions de protection des renseignements personnels qu'ils ont soulevées, m'ont obligé à attendre jusqu'à maintenant. Le Commissariat reviendra à son échéancier normal avec un rapport le printemps prochain.

Veuillez agréer, Monsieur, l'expression de mes sentiments les meilleurs.

Le Commissaire à la protection
de la vie privée du Canada,

George Radwanski

Table des Matières

Compte rendu sommaire du Commissaire 1

Première partie – Rapport concernant la *Loi sur la protection des renseignements personnels* 29

Introduction 29

Enquêtes 30

Plaintes en vertu de la *Loi sur la protection des renseignements personnels* 30

Définitions aux termes de la *Loi sur la protection des renseignements personnels* 34

Sommaire de cas choisis en vertu de la *Loi sur la protection des renseignements personnels* .. 35

Des renseignements personnels trouvés dans un conteneur à ordures au MDN 35

Des renseignements personnels détruits de façon prématurée à DRHC 36

Statistique Canada : préoccupations concernant la publication de renseignements sur certains groupes 37

Un nouveau système électronique à la Défense nationale a compromis la vie privée de milliers de personnes 39

Santé Canada ne sait pas si elle a communiqué des renseignements personnels 40

Des renseignements sur des permis de petite embarcation utilisés pour évaluer les taxes de vente 41

Absence de normes touchant la communication de renseignements personnels aux médecins 41

Les renseignements personnels d'un revendicateur du statut de réfugié communiqués à un autre revendicateur 43

Jurys de sélection et notes manuscrites 44

Le courrier électronique personnel n'est pas nécessairement privé 44

Incidents visés par la *Loi sur la protection des renseignements personnels* 47

L'ouverture du courrier – le droit à la vie privée doit être la première considération 47

Santé Canada et sa liste de présumés utilisateurs de marijuana 48

Vol de demandes remplies de permis d'armes à feu à Justice Canada 49

Des préoccupations au sujet d'une technologie d'identification biométrique 50

Une contribuable a reçu le remboursement d'une autre personne. 50

Communications dans l'intérêt public 51

Pratiques en matière de vie privée et examens 60

Introduction 60

Des renseignements personnels n'ayant pas été déchiquetés – Golden West Document Shredding, Inc. 61

Préoccupations en matière de vie privée du Programme canadien des armes à feu 65

Un nouveau protocole relatif aux bases de données est adopté suivant le Fichier longitudinal sur la main-d'œuvre 68

Examens 70

La Commission de l'immigration et du statut de réfugié et la Commission canadienne de sûreté nucléaire 70

Devant les tribunaux 70

Introduction 70

Décisions récentes 71

Le Commissaire à la protection de la vie privée c. le Conseil canadien des relations de travail 71

Le Commissaire à l'information du Canada (appelant) c. le Commissaire de la GRC (intimé) et le Commissaire à la protection de la vie privée (intervenant) ... 72

Affaires en instance 73

Formulaires de déclaration du voyageur (E-311) 73

Le Commissaire à la protection de la vie privée c. le Procureur général du Canada 73

Contestation en vertu de la Charte 74

Clayton Charles Ruby c. le Solliciteur général 76

Le Commissariat aux langues officielles (appelant) c. Robert Lavigne (intimé) 77

Deuxième partie – Rapport concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* 79

Introduction 79

Mise à jour des lois provinciales et territoriales 81

Détermination d'« essentiellement similaire » 81

Consentement 81

Critère de la personne raisonnable 82

Droits d'accès et de correction 82

Surveillance 82

Voies de recours 82
Initiatives législatives en vue de réglementer le secteur privé 82
Secteur de la santé 83
Loi pour le secteur privé 83
Enquêtes 83
Les Conclusions du Commissaire 84
Activités de surveillance vidéo dans un endroit public [principe énoncé à l'article 4.3 de l'annexe 1] 85
Messages électroniques non sollicités d'un fournisseur de services Internet [principe énoncé à l'article 4.3 de l'annexe 1] 86
Le Commissaire étudie le domaine de compétence dans une affaire de communication de renseignements d'une filiale bancaire à un tiers [article 30] .. 87
Une cliente d'une banque demande des renseignements sur sa cote de crédit [principe énoncé à l'article 4.9 de l'annexe 1, et article 8] 88
Conservation de renseignements personnels après le rejet d'une demande [principe énoncé à l'article 4.5 de l'annexe 1] 89
Sûreté du service téléphonique automatisé d'une banque [principe énoncé à l'article 4.7 de l'annexe 1] 90
Un musicien s'oppose à ce qu'une organisation professionnelle recueille des renseignements sur son salaire [article 2] 92
Utilisation et communication de renseignements personnels dans les annuaires téléphoniques [principe énoncé à l'article 4.3 de l'annexe 1] 93
Inscription du numéro de compte sur un chèque à la banque [paragraphe 5(3)] 94
Une entreprise de camionnage recueille des renseignements personnels prévus pour Douanes Canada [principe énoncé à l'article 4.4 de l'annexe 1] 96
Une banque perd des renseignements personnels concernant une cliente [principe énoncé à l'article 4.7 de l'annexe 1, et paragraphe 12(2)] 97
Un demandeur de carte de crédit s'oppose à la politique sur l'échange de renseignements d'une banque 98
Une banque accusée de retenir des certificats d'obligation [principe énoncé à l'article 4.9 de l'annexe 1, et article 8] 99
Vente de renseignements sur les habitudes de prescription des médecins [articles 2 et 3] . 100
Obstacles à la démarche d'un exécuteur testamentaire tâchant d'obtenir des renseignements concernant un coffre bancaire [principes énoncés aux articles 4.5 et 4.9 de l'annexe 1, et paragraphe 8(7)] 102
Un employé prétend que son employeur a communiqué sans son consentement des renseignements à une société de placement [paragraphe 7(3) et principes énoncés aux articles 4.3 et 4.5 de l'annexe 1] 103

Un demandeur affirme ne pas avoir reçu son rapport de solvabilité d'une agence d'évaluation [article 8] 104
Une entreprise de transport aérien accusée de priver des voyageurs de leur droit de consulter des renseignements personnels au sujet d'incidents de voyage [principes énoncés aux articles 4.1 et 4.9 de l'annexe 1] 105
Une employée s'oppose à ce que son employeur inscrive son numéro de compte bancaire sur sa fiche de paie [principes énoncés aux articles 4.3 et 4.7 de l'annexe 1] 107
Une entreprise demande le NAS d'une cliente en vertu d'une politique [principes énoncés aux articles 4.3.3 et 4.4.1 de l'annexe 1, et paragraphe 5(3)] ... 109
Une utilisatrice accuse un FSI de lire ses messages électroniques et d'empêcher leur transmission [principe énoncé à l'article 4.3 de l'annexe 1] 110
Un employeur envoie à des tiers des copies d'une réponse à des demandes d'accès présentées par une employée [principes énoncés aux articles 4.3 et 4.5 de l'annexe 1, et paragraphe 5(3)] 112
Une entreprise de téléphone demande des pièces d'identité aux nouveaux abonnés [principes énoncés aux articles 4.2 et 4.2.3 et aux articles 4.3, 4.3.2 et 4.3.3 de l'annexe 1, et paragraphe 5(3)] 114
Un radiodiffuseur accusé de recueillir des renseignements personnels avec son site Web [article 2, et principe énoncé à l'article 4.3 de l'annexe 1] 116
Un couple prétend que la banque lui a refusé l'accès à des renseignements sur une demande de prêt [paragraphes 8(3) et 8(5)] 117
Incidents en vertu de la *LPRPDÉ* 119
Une entreprise de transport recueille et communique des renseignements personnels concernant les passagers 119
Un site Web diffuse des conversations par téléphones cellulaires 120

Pratiques et examens en matière de vie privée 122

Devant les tribunaux 122
Mathew Englander c. Telus Communications Inc 122
Ronald G. Maheu c. le Procureur général du Canada et IMS Health Canada 123

Communications et sensibilisation du public 124
Documents de sensibilisation du public 125
Publicité 125
Site Web 125

Troisième partie – Services de gestion 127

Préparatifs pour la mise en œuvre de la loi pour le secteur privé 127

Structure organisationnelle 130

Compte rendu sommaire du Commissaire

Il s'agit de mon premier rapport à l'intention des Canadiens et Canadiennes à titre de Commissaire à la protection de la vie privée et je profite de l'occasion qui m'est offerte pour porter un regard en arrière et faire le bilan des réalisations de l'an dernier. En peu de temps, nous avons été témoins d'événements extraordinaires, à la fois technologiques et sociaux, qui ont comporté une incidence sans précédent sur la vie privée. [illegible], en ce qui me concerne personnellement, j'ai vécu une année remarquable remplie de découvertes.

Je me réjouis qu'au cours de la brève durée de mon mandat, plusieurs importantes victoires ont été remportées concernant les droits à la vie privée des Canadiens et Canadiennes :

- Le projet de loi antiterroriste du gouvernement fédéral a été modifiée de façon à assurer qu'il fait obstacle aux droits à la vie privée seulement lorsque cela est absolument nécessaire afin d'atteindre les objectifs légitimes en matière de sécurité. Dans sa version initiale, la Loi renfermait des dispositions qui dépassaient largement les objectifs fixés. Suivant ces dispositions, le Procureur général aurait été autorisé à retirer aux Canadiens et Canadiennes toute protection de la vie privée, dans la mesure où il l'aurait jugé indiqué, en délivrant des certificats globaux qui auraient abrogé la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques*. La ministre de la Justice a reconnu le bien-fondé de mes observations et a apporté des modifications qui ont tenu pleinement compte de mes réserves.

- L'ouverture du courrier en provenance de l'étranger par les agents de l'Agence des douanes et du revenu du Canada, pour le compte de Citoyenneté et Immigration Canada, a été limitée de façon à respecter davantage les droits à la vie privée. Cette ancienne pratique, fondée sur une distinction arbitraire et périmée entre le courrier et les colis en fonction du poids, énoncée dans la *Loi sur les douanes*, était parfaitement légale, tout en étant profondément viciée d'un point de vue de

George Radwanski
Commissaire à la protection de la vie privée du Canada

la vie privée. L'envoi du courrier dans de grandes enveloppes, comme l'exigent les services de messagerie prioritaire, faisait qu'il était suffisamment lourd pour ne plus être visé par l'exemption, qui consistait à protéger le courrier des Canadiens et Canadiennes de toute ouverture en l'absence d'un mandat. Suite à des discussions avec le ministre du Revenu national, ce dernier a fait en sorte que l'Agence révise ses procédures afin de respecter l'esprit de la loi. Lorsqu'on détermine le poids du courrier, on ne tient plus compte des enveloppes extérieures pour distinguer entre le courrier visé par les mesures de protection des renseignements personnels et les colis.

- On n'a pas donné suite à un projet de loi provincial profondément vicié sur la protection des renseignements personnels sur la santé en Ontario, qui aurait donné carte blanche au gouvernement provincial pour violer les droits à la vie privée en matière de santé. Parce que notre droit à la vie privée est indivisible – c'est-à-dire qu'il ne peut être respecté au fédéral et violé au provincial – j'ai accepté l'invitation de témoigner au sujet du projet de loi devant un comité de l'Assemblée législative. À l'encontre d'autres témoins qui ont recommandé des amendements, j'ai suggéré de retirer le projet de loi et de revenir à la case départ parce que la démarche qu'il proposait était fondamentalement défectueuse. Le projet de loi est resté en plan au Feuilleton. J'ai bon espoir que son substitut éventuel protégera réellement la vie privée.

Ces développements me portent à croire que la structure juridique canadienne en matière de vie privée, qui comprend un haut fonctionnaire du Parlement ou un ombudsman dont le mandat est de surveiller les droits à la vie privée des Canadiens et Canadiennes, est fondée et efficace. Avec le soutien suffisant du public, que l'on peut s'assurer en présentant les faits avec à-propos et persuasion, de grandes choses peuvent être réalisées et bon nombre de préjudices écartés.

J'ai assumé cette charge avec la détermination d'être un champion de la protection du droit à la vie privée de tous les Canadiens et de toutes les Canadiennes. Pour ce faire, j'ai cru bon de revigorer le Commissariat à la protection de la vie privée et de sensibiliser davantage les Canadiens et Canadiennes aux questions touchant la vie privée qui ont une incidence sur leur vie.

Par conséquent, l'effectif du Commissariat a presque doublé depuis l'an dernier. Lorsque je suis entré en fonction en septembre 2000, celui-ci comptait 54 employés. Au 30 novembre 2001, le personnel s'était accru et totalisait 84 (97 si l'on comprend la Direction générale des services de gestion intégrée). Cet accroissement visait deux objectifs : nous acquitter de nos nouvelles responsabilités de surveillance aux termes de la *Loi sur la protection des*

LA VIE PRIVÉE EST MENACÉE COMME ELLE NE L'A JAMAIS ÉTÉ AUPARAVANT.

renseignements personnels et les documents électroniques, qui est entrée en vigueur en janvier; et créer la direction des communications qui joue un rôle clé en vue de sensibiliser davantage au droit fondamental à la vie privée.

La conscientisation du public est une composante indispensable du rôle que je suis appelé à jouer. En tant qu'ombudsman, je dispose de deux mécanismes fondamentaux : la persuasion et la publicité. Il est bien évident que la persuasion est grandement rehaussée si elle est appuyée, dans la mesure du possible, d'une opinion publique avertie et alerte.

Les Canadiens et Canadiennes doivent connaître et comprendre leurs droits à la vie privée et exiger que ceux-ci soient pleinement respectés. C'est pourquoi, depuis mon entrée en fonction, j'ai accordé une importance primordiale à mes responsabilités de communicateur. Jusqu'à date, j'ai prononcé 35 discours à divers auditoires partout au Canada, et accordé plus de 210 entrevues aux médias.

Bien entendu, avant d'être nommé, j'étais sensibilisé au fait que la vie privée constitue un enjeu important. J'étais conscient qu'il s'agissait d'un élément essentiel d'une société libre, et j'ai convenu avec l'ancien juge LaForest de la Cour suprême que la vie privée se trouvait « au cœur de la liberté dans un État moderne ». [traduction libre] Et le postulat, à savoir que la vie privée est le droit le plus fondamental duquel émanent toutes les libertés – la liberté de parole, la liberté d'association, la liberté de choix, pour ne nommer que celles-là –, m'a frappé en raison de sa justesse.

Mais je me suis vite rendu compte dans l'exercice de ma charge que la vie privée était encore beaucoup plus importante, et sa protection plus urgente, que ce que j'avais escompté.

Il s'agit d'une période critique en tant que Commissaire à la protection de la vie privée. La vie privée est menacée comme elle ne l'a jamais été auparavant. Par le passé, on a souvent sonné le glas de la vie privée. Mais il est triste de dire que ce son d'alarme a été rejeté par de nombreuses personnes parce qu'elles y voyaient une exagération.

Aujourd'hui, une personne assez bien informée ne peut plus se permettre de le rejeter. Les moyens technologiques qui peuvent supprimer la vie privée sont en place, et pas seulement les ordinateurs et la technologie de traitement des renseignements, mais aussi la panoplie de sorcelleries technologiques allant des caméras vidéo, aux logiciels de reconnaissance de visage et aux cartes d'identité « intelligentes ». Et les motifs pour le faire existent bel et bien, et il ne s'agit pas nécessairement de motifs ignobles. En effet, les plus grandes menaces à la vie privée ne sont souvent pas posées par les personnes qui veulent y porter atteinte, mais bien par celles qui soutiennent avec la plus grande conviction que la vie privée doit être sacrifiée à quelque bien plus important.

Bon nombre d'entre nous pouvons maintenant envisager un monde sans vie privée, pas seulement l'envisager, mais aussi le présager comme probable et imminent, dans un avenir que nous verrons. Nous n'avons pas besoin d'un George Orwell pour nous dire « Tâchez d'imaginer ce qu'il en serait ». [traduction libre] Nous commençons tous à le voir autour de nous.

Nous faisons maintenant face à la possibilité réelle de devoir vivre en surveillant nos arrières, soit métaphoriquement, soit littéralement. Nous pouvons tous envisager une situation réelle et imminente dans laquelle il nous faudra peser chaque geste, chaque transaction, chaque déclaration, voire chaque contact humain, en pensant à qui en prendra connaissance, les jugera, les interprétera faussement ou les utilisera à notre détriment.

Est-ce là la liberté? Bien au contraire, il s'agit d'une réalité propre aux sociétés totalitaires.

Pourtant, je m'inquiète à l'idée que de nombreux Canadiens et Canadiennes soient au courant de l'atteinte à leur vie privée sans toutefois se rendre compte de son ampleur. Ils y portent attention seulement lorsque leur propre vie privée a été violée, lorsqu'il est déjà trop tard. Une fois que la vie privée a été violée, celle-ci ne peut jamais être pleinement rétablie. Lorsque les renseignements personnels de l'un d'entre nous sont révélés à une personne qui n'a pas affaire à les connaître, il est impossible de faire que cela soit autrement.

Les pressions exercées sur les droits à la vie privé ont de toute évidence été accusées dans la foulée des attaques terroristes du 11 septembre. Lorsque règne un climat de peur et d'incertitude, il devient facile de croire que plus l'État détient de renseignements à notre sujet, plus en sécurité nous serons. Cela, en retour, peut conférer une nouvelle légitimité injustifiée à ce qui pose justement les plus grandes menaces à la vie privée, par exemple, la prolifération de la surveillance vidéo, l'utilisation généralisée de la technologie de reconnaissance biométrique ou les cartes d'identité nationales.

Ces pressions s'intensifient parce qu'un climat de crainte fraye la voie non seulement aux intrusions dans la vie privée, mais tend également à décourager ou à sanctionner la dissidence. À la lumière de la destruction semée par les terroristes, quiconque s'oppose aux mesures qui même semblent vaguement rehausser la sécurité, doit accepter de courir le risque d'être accusé d'irresponsabilité.

Pourtant, le monde a toujours été un endroit dangereux, et l'évolution des droits fondamentaux, comme le droit à vie privée, nous enseigne que leur plus grande valeur découle de leur pérennité et de leur capacité de nous protéger en période d'adversité. Lorsqu'il n'y a pas de raison contraignante de violer un droit, nous le percevons non en tant que droit mais comme un fait de la vie. C'est seulement lorsque nous voulons poursuivre un but que

> SI NOUS RÉAGISSONS AU TERRORISME EN NOUS PRIVANT DE FAÇON EXCESSIVE ET INUTILEMENT DE NOTRE DROIT À LA VIE PRIVÉE ET DES LIBERTÉS QUI EN DÉCOULENT, LE TERRORISME AURA ALORS REMPORTÉ UNE GRANDE ET TERRIBLE VICTOIRE.

nous estimons irrésistible en faisant fi de toute autre considération, que l'engagement de notre société à la protection des droits fondamentaux est vraiment mis à l'épreuve.

La vie privée et les autres libertés et valeurs précieuses qui définissent la société canadienne ne sont pas des frivolités ou des luxes dans la situation que nous vivons depuis le 11 septembre. Plutôt, ce sont les enjeux les plus importants dans une telle situation. Si nous réagissons au terrorisme en nous privant de façon excessive et inutilement de notre droit à la vie privée et des libertés qui en découlent, le terrorisme aura alors remporté une grande et terrible victoire.

Au dire de tous, l'objet visé par la campagne terroriste maintenant en cours est d'attaquer et de miner la nature même de la société américaine et, partant, de toutes les sociétés démocratiques. Cela fait que nos libertés et valeurs, et surtout la vie privée, sont les plus importantes cibles. Toute restriction inconsidérée de ces libertés et toute atteinte déplacée à la vie privée, au lieu d'accroître notre sentiment de sécurité, montreraient que le terrorisme atteint ses objectifs et présente une occasion de fomenter la terreur.

Mon rôle à titre de Commissaire à la protection de la vie privée est de faire tout en mon pouvoir pour assurer que le droit humain et la valeur canadienne fondamentale, la vie privée, ne succombent pas au terrorisme.

En m'acquittant de cette responsabilité, je ne soutiens pas que le droit à la vie privée est un droit absolu ou encore que certaines mesures intrusives ne sont pas nécessaires en réponse aux menaces à la sécurité auxquelles nous faisons maintenant face.

Il reste qu'il est de mon devoir d'insister pour que nous décidions toujours de telles mesures avec calme, circonspection et au cas par cas, et que celles-ci doivent être justifiées suivant des critères clairs. J'ai recommandé les critères suivants à la fois pour les gouvernements et le secteur privé :

- Toute mesure proposée pour limiter le droit à la vie privée ou empiéter sur celui-ci doit être nécessaire afin d'aborder un problème particulier.
- La mesure doit être efficace pour régler le problème, autrement dit, il doit être démontré que celle-ci accroîtra le niveau de sécurité et non seulement notre sentiment de sécurité.
- Le degré d'intrusion dans la vie privée et de limitation de celle-ci doit être proportionnel à l'avantage en matière de sécurité qui en découlera. Autrement dit, il ne faut pas utiliser un marteau pour tuer un moustique.
- Enfin, il ne peut y avoir de mesures moins intrusives qui permettraient d'atteindre les mêmes résultats.

Bien que certaines difficultés initiales aient été éprouvées, la réponse législative du gouvernement fédéral à la menace de terrorisme satisfait aux critères énoncés ci-dessus concernant les droits à la vie privée. Je crois que cette réponse a permis d'établir un équilibre raisonnable et prudent entre la sécurité et la vie privée. Je continue à mettre de l'avant mes réserves et recommandations quant aux mesures législatives à venir.

Au cours des prochains mois, il ne fait aucun doute que d'autres difficultés et menaces relatives à la vie privée se présenteront dans la foulée des événements du 11 septembre. Les choix que nous ferons revêtiront une importance considérable.

Au cours des jours et des semaines qui ont suivi les attaques, le public a pris connaissance des questions qui inquiétaient depuis longtemps les défenseurs des droits à la vie privée. Il s'est rendu compte que de vastes intérêts industriels sont impatients de fabriquer et de vendre la technologie de surveillance : les caméras vidéo, les systèmes de reconnaissance de visage, les lecteurs d'empreintes digitales, les dispositifs de surveillance du courrier électronique et de sites Web, les cartes d'identité « intelligentes », et les systèmes de repérage. Et il a vu qu'un grand nombre de personnes sont prêtes à soutenir que quiconque n'a rien à cacher à son sujet ne devrait pas s'opposer à tout révéler.

Depuis l'an dernier, bien avant les tragiques événements du 11 septembre, je me suis rendu à l'évidence que la vie privée serait une question déterminante de la nouvelle décennie. C'est un message que j'ai maintes fois répété au cours de mes communications publiques. Jusqu'à récemment, ce que je voulais dire, c'est que nous faisons face à des choix sans précédent et irrévocables touchant la vie privée en raison des percées technologiques et scientifiques, et que ces choix détermineront la qualité de notre vie.

Cela demeure vrai, mais maintenant plus que jamais, la vie privée sera une question décisive parce que les décisions que nous prendrons concernant l'équilibre entre la sécurité et la vie privée détermineront le genre de société que nous léguerons à nos enfants et à nos petits enfants. Même une société orwellienne exempte de vie privée ne serait entièrement sûre – même un État policier le plus tyrannique qui soit n'est pas à l'abri du terrorisme – mais le fait de nous désinvestir graduellement de nos droits à la vie privée dans l'intérêt de la sécurité éliminerait en retour de notre vie la dignité et la liberté qui sont les gages de notre société.

En rétrospective, nous verrons inévitablement cette décennie comme celle où nous avons eu l'occasion d'affirmer la valeur cruciale de la vie privée et de la défendre contre ses assaillants. J'espère fermement que nous serons capables de nous souvenir de cette décennie comme de celle où nous avons saisi cette occasion et franchi un pas décisif.

> JE PRÉFÈRE TOUTEFOIS UNE DÉFINITION PLUS MODERNE ET PEAUFINÉE DE LA VIE PRIVÉE EN TANT QUE DROIT D'EXERCER UN CONTRÔLE SUR L'ACCÈS À SES RENSEIGNEMENTS PERSONNELS AINSI QU'À SA PERSONNE.

Autrefois, la majorité des personnes définissaient la vie privée en employant une variante de la célèbre formule de Samuel Warren et de Louis D. Brandeis, comme « le droit de ne pas être dérangé ». [traduciton libre] Il s'agit toujours d'une définition valable et elle reflète assurément l'importance viscérale que les gens accordent à la vie privée.

Je préfère toutefois une définition plus moderne et peaufinée de la vie privée en tant que droit d'exercer un contrôle sur l'accès à ses renseignements personnels ainsi qu'à sa personne. Cette définition permet de mieux saisir la nature des menaces modernes posées à la vie privée, qui se présentent surtout dans le contexte de la collecte et de l'utilisation des renseignements à notre sujet.

C'est pourquoi j'ai dit si souvent au cours de l'année dernière que nous sommes à la croisée des chemins. Ce que je veux dire, c'est que les moyens que nous avons pris pour protéger la vie privée par le passé, plutôt les moyens qui permettaient d'assurer sa protection sans que nous nous en occupions, ne sont plus aussi efficaces et ils le seront de moins en moins avec le temps.

Déjà la protection de la vie privée était plus ou moins assurée « par défaut ». Lorsque les dossiers imprimés qui renfermaient des renseignements nous concernant étaient éparpillés à de nombreux endroits, la constitution d'un dossier détaillé sur n'importe quel individu était une tâche ardue. À moins d'être célèbre, important ou soupçonné d'une infraction grave, la vie privée pouvait être relativement sûre sans devoir déployer beaucoup d'efforts pour s'en assurer.

L'avènement de la tenue électronique de dossiers a changé tout cela, éliminant les obstacles liés au temps, à la distance et au coût qui assuraient déjà notre vie privée. De nouvelles technologies de surveillance : les témoins et les dispositifs d'écoute sur le Web, les caméras vidéo, la surveillance du courrier électronique, les cartes intelligentes, les identificateurs biométriques, les dispositifs de repérage, les tests de dépistage de drogues, nous assaillent où que nous soyons. Des étrangers assis à leur ordinateur dressent des dossiers complets sur nous en quelques secondes. Nos activités et nos intérêts, nos achats et nos déplacements, nos opinions et nos habitudes sont consciencieusement consignés, analysés et classés pour quelque usage auquel le plus offrant veut les destiner.

Maintenant que la protection « par défaut » disparaît, il nous revient de prendre la barre.

Comme je l'ai mentionné ci-dessus, un des faits les plus intéressants que j'ai observé l'an dernier est que les plus grandes menaces à la vie privée viennent rarement des personnes qui veulent y porter atteinte.

« IL FAUT VOIR LA VIE PRIVÉE, NON COMME UN INTÉRÊT INDIVIDUEL ÉGOÏSTE QUI DOIT CÉDER LA PLACE AUX BESOINS SOCIAUX PLUS IMPORTANTS, MAIS BIEN COMME UN INTÉRÊT SOCIAL, COMMUN ET COLLECTIF, CE QU'IL EST DE FAIT.

Ces menaces viennent de personnes bien intentionnées qui affirment que la vie privée doit être sacrifiée à quelque bien supérieur – le service à la clientèle amélioré, la prévention de la criminalité, l'avancement de la science, la prestation plus efficace de programmes gouvernementaux, la sécurité.

Bien entendu, il arrive parfois que la vie privée cède le pas à d'autres intérêts sociaux.

Mais il nous faut nous demander, et demander à ces personnes bien intentionnées, quel genre de société nous desservirons, construirons et appuierons si la suppression de la vie privée est le prix que nous nous apprêtons à payer si volontiers.

Il faut voir la vie privée, non comme un intérêt individuel égoïste qui doit céder la place aux besoins sociaux plus importants, mais bien comme un intérêt social, commun et collectif, ce qu'il est de fait.

Voilà pourquoi c'est une importante période pour le Commissaire à la protection de la vie privée.

Il s'agit également d'une période importante pour une nouvelle loi sur la protection de la vie privée pour le secteur privé. Pendant près de 20 ans, nous avions une loi qui régissait la façon dont les gouvernements recueillaient et traitaient les renseignements personnels des Canadiens et Canadiennes. Mais c'est maintenant le secteur privé qui connaît une explosion d'activités de collecte de renseignements et de constitution de dossiers personnels. Et c'est là où il faut de toute urgence exercer un contrôle sur les renseignements personnels.

Le Parlement a adopté la *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*) il y a près de deux ans, et celle-ci est entrée en vigueur le 1er janvier 2001. La *Loi* constitue un important outil qui permettra aux Canadiens et Canadiennes d'exercer de nouveau un contrôle sur leurs renseignements personnels et de s'intéresser à protéger et à préserver leur vie privée.

La *Loi* vise les renseignements personnels recueillis, utilisés ou communiqués dans le cadre des activités commerciales. Elle repose sur un code modèle de protection des renseignements personnels, qui a été élaboré conjointement par les entreprises, le gouvernement et les groupes de consommateurs. Le code est fondé sur des principes largement reconnus liés à des pratiques équitables en matière de renseignements, y compris ceux établis par l'Organisation de la coopération et du développement économiques en 1980.

En bref, la *Loi* porte ce qui suit :

- Hormis certaines exceptions fort limitées, il est interdit aux organisations du secteur privé de recueillir, d'utiliser ou de communiquer vos renseignements personnels sans votre consentement.

- L'organisation peut recueillir, utiliser ou communiquer vos renseignements seulement pour les fins auxquelles vous avez consenti.
- Même avec votre consentement, l'organisation peut seulement recueillir les renseignements qu'une personne raisonnable estimerait acceptables dans les circonstances.
- Les personnes ont le droit d'accéder aux renseignements personnels qui sont détenus à leur sujet et de corriger toute inexactitude.
- Le Commissariat et moi-même exerçons une surveillance de façon à assurer le respect de la *Loi*. Des mesures de recours sont offertes aux personnes dont les droits ont été violés.

La *Loi* entre en vigueur en étapes successives. Elle s'applique depuis janvier 2001 aux renseignements personnels, à l'exception des renseignements sur la santé, des clients ou des employés d'entreprises de compétence fédérale, surtout les banques, les entreprises de télécommunications, de radiodiffusion et de transport interprovincial ou international, ainsi que celles dans les Territoires du Nord-Ouest, du Yukon et du Nunavut, où la *Loi* s'applique au secteur privé qui, aux termes de la Constitution, est réglementé par le fédéral.

La *Loi* vise également les renseignements personnels – de nouveau, autres que ceux sur la santé – lorsque ceux-ci sont communiqués à l'extérieur d'une province ou du pays pour contrepartie. Dans le jargon juridique, « communiqué pour contrepartie » signifie qu'on obtient quelque chose en échange des renseignements, par exemple, dans le cadre de ventes, de locations ou d'échanges. Les renseignements personnels eux-mêmes doivent faire l'objet d'un échange pour que la *Loi* soit applicable.

L'exclusion des renseignements personnels sur la santé était un compromis de dernière minute et n'est que temporaire.

Lorsque la *Loi* suivait le processus parlementaire, des représentants du secteur de la santé ont soulevé deux ensembles distincts et opposés de préoccupations. Certains voulaient une loi plus sévère, assortie de dispositions en matière de consentement plus contraignantes et des restrictions sur l'utilisation ultérieure des renseignements personnels sur la santé. D'autres étaient d'avis que la *Loi* restreindrait les activités opérationnelles dans le milieu de la santé et voulaient qu'elle soit plus permissive.

Pourtant, il n'y avait pas de problèmes ou d'obstacles fondamentaux à surmonter. Tout le monde reconnaissait que les renseignements personnels sur la santé devaient être protégés. À ce temps-là et depuis, personne n'a présenté d'indications claires et particulières pourquoi

« LES RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ, QUI PORTENT SUR L'ÉTAT DE NOTRE CORPS ET DE NOTRE ESPRIT, SONT, COMME ON PEUT LE SOUTENIR, LES PLUS PRIVÉS DE TOUS.

la *Loi*, telle qu'elle était libellée, ne pouvait être efficace. En effet, comme l'a indiqué le ministre de la Santé d'alors, David Dodge, lors de sa comparution devant un comité du Sénat :

> Cela fait environ six mois que je demande des renseignements précis sur ce qui pourrait déraper si le projet de loi était adopté, tel que prévu dans un an. J'ai exercé des pressions afin de déterminer les choses qui pourraient ne pas fonctionner et ce que nous ne pourrions faire. Franchement, j'ai été surpris que malgré les critiques générales et l'incertitude, je n'ai toujours pas eu d'exemples de choses qui pourraient mal tourner. Parce que nous sommes en territoire inconnu, il en découle des doutes et de l'incertitude. Toutefois, on ne m'a toujours pas fourni d'exemples de choses qui pourraient de fait mal tourner. [traduction libre]

On a éventuellement convenu d'exclure les renseignements sur la santé de la *Loi* durant une période d'un an après son entrée en vigueur, de façon à accorder au secteur de la santé suffisamment de temps pour s'adapter à la nouvelle *Loi*.

Récemment, des efforts de lobbying déterminés ont été déployés par divers intérêts puissants du secteur de la santé pour continuer à priver les Canadiens et Canadiennes de la protection des renseignements personnels sur la santé, dont l'entrée en vigueur était prévue pour le 1er janvier. Certains ont exercé des pressions pour qu'on prolonge l'exclusion des renseignements personnels sur la santé. D'autres encore aimeraient que la *Loi* soit modifiée de diverses façons, notamment en adoptant un régime réglementaire distinct qui passerait outre aux dispositions de la *Loi* et éliminerait le rôle de surveillance joué par le Commissaire à la protection de la vie privée.

Mais deux choses sont demeurées constantes depuis l'an dernier. Tout d'abord, on n'est toujours pas parvenu à recueillir un large consensus, car certains sont toujours favorables à une loi plus sévère, tandis que d'autres veulent l'affaiblir. En second lieu, personne n'est encore parvenu à démontrer de façon précise et persuasive ce qui cloche avec le libellé de la *Loi*.

À mon avis, tout délai ou affaiblissement de la protection des renseignements personnels sur la santé, à laquelle s'attendent les Canadiens et Canadiennes comme leur a promis le Parlement, représenterait un terrible coup porté aux droits à la vie privée.

Les renseignements personnels sur la santé, qui portent sur l'état de notre corps et de notre esprit, sont, comme on peut le soutenir, les plus privés de tous. Toute communication indue peut comporter des conséquences dévastatrices. En effet, la crainte de ne plus pouvoir exercer de contrôle sur leurs

renseignements personnels sur la santé peut empêcher des personnes de demander des soins médicaux, ce qui comporterait des résultats préjudiciables non seulement pour ces personnes mais également pour la société dans son ensemble. C'est pourquoi, une loi sur la protection de la vie privée qui ne garantit pas pleinement la protection des renseignements personnels sur la santé n'est pas acceptable. La prorogation d'un an accordée à cet égard est plus que suffisante.

Une inquiétude encore plus grande tient au fait que tout délai ou affaiblissement de la protection des renseignements personnels sur la santé réduise l'efficacité de la LPRPDÉ dans l'ensemble. Les intervenants du milieu de la santé peuvent soutenir que leur secteur est visé par des questions spéciales et distinctes en matière de vie privée. Mais les intervenants du milieu bancaire, des transports et des télécommunications, somme toute de n'importe quel secteur de l'économie, pourraient facilement soutenir le même argument.

C'est pourquoi, la *Loi* a été rédigée sur la base de principes et de règles relativement larges, en accordant une marge de manœuvre et une interprétation fort amples relativement à son application. Si des exceptions spéciales devaient être accordées à un secteur, comme celui de la santé, tous les autres secteurs pourraient demander un traitement de faveur, et toute la structure sur laquelle repose la *Loi sur la protection des renseignements personnels* s'écroulerait.

J'ai été très heureux d'apprendre que le ministre de la Santé, l'honorable Allan Rock, abondait dans mon sens dans une lettre du 24 septembre qu'il m'a envoyée :

> Je n'appuie pas la création d'un organisme de réglementation distinct qui se chargerait des renseignements personnels sur la santé aux termes de la *LPRPDÉ*. La *Loi*, qui a été adoptée par le Parlement il y a un peu plus d'un an, énonce clairement que la surveillance, les mesures de réparation et les responsabilités en matière de vérification reviennent au Commissaire à la protection de la vie privée. Le sous-ministre a également clairement indiqué aux intervenants du secteur de la santé que nous n'envisageons pas de modifications à la *LPRPDÉ* en vue de créer un organisme distinct pour le secteur de la santé, et que nous n'appuyons pas de prorogation de l'application de la *LPRPDÉ* au secteur de la santé. [traduction libre]

Je suis reconnaissant au ministre de la Santé d'avoir reconnu, pour le compte de son ministère, l'importance vitale de l'entrée en vigueur de la protection des renseignements personnels sur la santé, telle que prévue le 1er janvier 2002.

« IL EST IMPORTANT DE SOULIGNER QU'IL RESTE DEUX ANS AU SECTEUR DE LA SANTÉ POUR SE PRÉPARER À L'ENTRÉE EN VIGUEUR DE LA *LOI* DANS LES DOMAINES QUI LE PRÉOCCUPENT LE PLUS.

Au moment de rédiger le présent rapport, il semblait en effet que la *Loi* sera appliquée telle qu'elle a été libellée. Le 1er janvier 2002, les renseignements personnels sur la santé détenus par les entreprises fédérales sur leurs clients ou employés seront protégés.

La vente ou l'échange de renseignements personnels sur la santé à l'extérieur d'une province ou du pays est également visé par la *Loi*. La communication de renseignements personnels sur la santé au-delà des territoires pour contrepartie (dans la mesure où la contrepartie vise les renseignements) sera couverte. En outre, toutes les entreprises et les organisations au Yukon, dans les Territoires du Nord-Ouest et au Nunavut qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre de leurs activités commerciales devront également assurer la protection des renseignements personnels sur la santé.

Il est important de souligner qu'il reste deux ans au secteur de la santé pour se préparer à l'entrée en vigueur de la *Loi* dans les domaines qui le préoccupent le plus. Ainsi, la *Loi* s'appliquera seulement directement aux services commerciaux touchant la santé, tels que ceux fournis par les cabinets de médecin, les cliniques privées, les laboratoires et les pharmacies, que le 1er janvier 2004. À cette date, la *Loi* s'appliquera à toutes les activités commerciales du secteur privé dans les provinces, sauf lorsqu'une province a adopté une loi essentiellement similaire.

J'aimerais aborder une question particulière à ce point-ci.

Je sais que les intervenants du milieu de la santé sont préoccupés à juste titre au sujet de l'incidence possible de la *Loi* sur la recherche sur la santé, car elle vise des renseignements personnels sur la santé et des considérations pécuniaires qui peuvent être en cause. J'aimerais préciser que la recherche sur la santé en bonne et due forme, qui est entreprise avec sensibilité relativement aux droits à la vie privée des Canadiens et Canadiennes, n'a rien à craindre de la *Loi* ou du Commissariat.

Ma position sur cette importante question est la suivante :

Les renseignements personnels sur la santé représentent sans doute les renseignements personnels de nature la plus hautement délicate touchant la vie privée et, en règle générale, les individus doivent pouvoir exercer un droit de regard sur les personnes qui peuvent recueillir, utiliser ou communiquer ces renseignements ainsi que les fins pour lesquelles elles le font. Parallèlement, toutefois, notre société s'intéresse à juste titre à la poursuite et à l'accroissement de la recherche sur la santé, qui promet d'importants bénéfices à tous les individus.

La clause sur l'objet de la *Loi* précise que les règles visent à équilibrer le « droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir,

d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances ».

Concernant la recherche sur la santé, il me semble qu'il soit clair qu'un juste équilibre permet de protéger les intérêts authentiques des individus en matière de vie privée, tout en permettant la conduite de recherches légitimes sur la santé, qui utilisent les renseignements sans comporter d'incidence possible sur les individus auxquels ils se rapportent. Je ne crois pas que l'objet de la *Loi* était d'empêcher ou d'entraver de quelque façon que ce soit la recherche, et mes homologues provinciaux et territoriaux avec qui j'ai discuté de cette question cet été partageaient mon avis.

Par conséquent, j'ai l'intention d'interpréter largement l'objet de l'alinéa 7(2)c) de la *Loi* qui autorise une organisation à utiliser les renseignements personnels à l'insu de l'intéressé et sans son consentement dans la mesure où « l'utilisation est faite à des fins statistiques ou à des fins d'étude ou de recherche érudites, ces fins ne peuvent être réalisées sans que le renseignement soit utilisé, celui-ci est utilisé d'une manière qui en assure le caractère confidentiel, le consentement est pratiquement impossible à obtenir et l'organisation informe le Commissaire de l'utilisation avant de la faire ». L'alinéa 7(3)f) comprend une disposition parallèle visant la communication des renseignements personnels à l'insu de l'intéressé ou sans son consentement.

Je suis d'avis que la recherche sur la santé authentique entreprise par des organisations dûment agréées et qui est assortie de mesures de sauvegarde indiquées représente de fait une étude ou une recherche statistique ou savante, et ce, que des intérêts pécuniaires soient engagés ou non. Du simple fait que la recherche sur une condition médicale donnée puisse bénéficier d'une aide au financement d'une source extérieure, qui espère tirer des gains financiers de la découverte d'un nouveau médicament efficace, par exemple, ne modifie nullement à mon avis sa légitimité en tant que recherche sur la santé d'un point de vue des droits à la vie privée.

Concernant l'impossibilité d'obtenir un consentement pour une telle recherche, je reconnais le bien-fondé de la position du milieu de la recherche sur la santé, à savoir que des facteurs de coûts ou la difficulté d'obtenir le consentement auprès de 100 % de la population cible font qu'il est impraticable d'obtenir le consentement individuel pour bon nombre d'études sur la santé.

La *Loi* exige que les renseignements en question soient utilisés de façon à en assurer la confidentialité. Je crois que cette exigence est d'importance primordiale.

J'adopterai en conséquence la position selon laquelle les renseignements personnels sur la santé peuvent être communiqués et utilisés sans consentement aux fins de la recherche sur la santé décrite ci-dessus, mais seulement dans

« Bref, nous jouirons bientôt d'une protection homogène de la vie privée au Canada.

la mesure où ceux-ci sont strictement confinés par le projet de recherche et que les individus qu'il concerne ne subissent aucun préjudice.

Sans restreindre la portée générale de ce qui précède, je considère comme une exigence absolue que la communication et l'utilisation des renseignements personnels sur la santé sans le consentement des personnes visées, aux fins de la recherche sur la santé, ne peuvent de quelque façon que ce soit parvenir à l'employeur, à l'assureur, aux parents ou aux connaissances de l'individu, ni aux autorités gouvernementales ou aux forces de l'ordre, aux mercaticiens ou à tout autre tiers. Il est en outre interdit à quiconque, autre que le médecin de l'individu ou tout autre fournisseur principal des soins de santé, le cas échéant, de communiquer avec l'individu en raison de ces renseignements.

Le Commissariat et moi-même assurerons une surveillance vigilante de cette exigence, et tout manquement sera considéré, de plein droit, comme une violation extrêmement grave de la *Loi*.

Je suis convaincu que cette démarche satisfera pleinement l'esprit de la *Loi*, permettra de protéger efficacement les droits à la vie privée des Canadiens et Canadiennes, et toute recherche légitime sur la santé pourra être menée sans entrave.

La dernière étape de la mise en œuvre de la *Loi* débutera en janvier 2004. À ce temps-là, celle-ci visera toutes les activités commerciales au Canada, sous réserve d'une importance exemption : lorsqu'une province a adopté une loi sur la vie privée essentiellement similaire, le gouvernement fédéral peut exempter les organisations et les activités dans la province de l'application de la loi fédérale, et la loi provinciale aura préséance.

Les entreprises réglementées par le fédéral dans ces provinces continueront d'être régies par la *Loi* fédérale ainsi que les échanges de renseignements personnels entre les organisations à l'extérieur d'une province ou à l'étranger dans le cadre de leurs activités commerciales.

Bref, nous jouirons bientôt d'une protection homogène de la vie privée au Canada. Tout le secteur privé devra se conformer à la loi fédérale ou à une loi provinciale essentiellement similaire.

Une des remarques au sujet de la nouvelle loi pour le secteur privé que j'ai faite fréquemment l'an dernier, surtout devant des auditoires de gens d'affaires, est que la *Loi* ne démarque pas le Canada du reste du monde. Des lois semblables ont été adoptées dans la majorité des pays les plus évolués d'un point de vue économique, à l'exception des États-Unis. Même là, le débat porte moins sur les principes que sur la meilleure façon de les observer.

J'AI DÉCIDÉ DÈS LE DÉPART DE METTRE UN ACCENT SPÉCIAL SUR LA COMMUNICATION.

Une des raisons pour lesquelles ce genre de loi est adoptée est que lorsqu'un pays en a promulgué une, il ne peut assurer l'entière protection des renseignements de ses citoyens que si les pays avec lesquels il fait des échanges offrent une protection semblable. Afin de favoriser une meilleure compréhension de notre façon de protéger la vie privée au Canada, j'ai prononcé des discours et participé à des conférences à Washington, à l'Université Harvard, ainsi qu'à Bruxelles, à Cambridge et à Londres, et je me suis entretenu avec des commissaires à la protection de la vie privée et aux données nominatives partout sur la planète.

Lorsque j'ai été nommé Commissaire à la protection de la vie privée, j'ai examiné la situation qui existait, c'est-à-dire les multiples menaces à la vie privée qui découlaient d'objectifs sociaux raisonnables, les attentes de plus en plus limitées face à la vie privée, une nouvelle loi complexe, et un public qui, dans une certaine mesure, semblait tellement habitué à voir sa vie privée s'amenuiser qu'il courait le risque de perdre de vue la signification et l'importance de celle-ci.

Compte tenu de tout cela, j'ai décidé dès le départ de mettre un accent spécial sur la communication.

Une des premières mesures que j'ai prises en tant que Commissaire à la protection de la vie privée a été de créer la Direction des communications et des analyses stratégiques au sein du Commissariat, qui serait chargée de mener des recherches sur les questions touchant la vie privée et de joindre le public afin de le renseigner et d'obtenir ses avis. Et j'ai personnellement saisi toutes les occasions qui m'étaient offertes de transmettre mon message, me rendant aux quatre coins du pays, prenant la parole lors de conférences et de réunions, et accordant des entrevues aux médias.

J'ai également veillé à ce que le public ait accès à des renseignements exacts et courants sur notre site Web. Les discours, par exemple, que je prononce y sont affichés en version publiée dès que je les ai livrés. Nous avons fait paraître des trousses d'information sur des sujets variés, y compris le vol d'identité, le recensement et, bien entendu, comment accéder aux renseignements personnels et faire valoir ses droits aux termes des lois canadiennes sur la vie privée. Nous avons également publié des guides complets à l'intention des individus et des entreprises sur la nouvelle loi et son incidence sur ces derniers.

J'ai fait tout cela parce qu'il est très important que les Canadiens et Canadiennes soient bien renseignés sur leurs droits et qu'ils comprennent les implications de la perte de leur vie privée. Et en bout de ligne, je dois avouer que je compte sur l'appui du public dans mon rôle d'ombudsman, qui est mon principal recours afin d'assurer la protection des droits

« L'AN DERNIER, LES ACTIVITÉS DE SURVEILLANCE SE SONT ACCRUES, À LA FOIS PAR LES GOUVERNEMENTS ET LE SECTEUR PRIVÉ, CE QUI A PLACÉ CETTE QUESTION À L'AVANT-PLAN DE NOS PRÉOCCUPATIONS.

des Canadiens et Canadiennes aux termes de la *Loi sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels et les documents électroniques.*

Je ne suis pas investi de pouvoirs officiels en vue de contraindre les institutions fédérales et les entreprises du secteur privé à respecter la vie privée des personnes, ou à faire réparation à ces dernières de tout manquement. Je peux faire appel aux tribunaux dans certaines situations, bien entendu, mais ce n'est jamais une solution optimale. Je fais surtout appel au pouvoir qu'exerce l'opinion publique. Peu de personnes, que ce soit dans les gouvernements ou les entreprises, veulent mécontenter le public. D'ailleurs, plus le public est mieux informé, plus son opinion sera respectée.

J'aimerais maintenant revenir, comme j'ai dit que je le ferais, à certaines questions précises touchant la vie privée qui m'ont interpellé cette année.

La surveillance – la surveillance visuelle factuelle – a longtemps été une principale préoccupation des défenseurs des droits à la vie privée. L'an dernier, les activités de surveillance se sont accrues, à la fois par les gouvernements et le secteur privé, ce qui a placé cette question à l'avant-plan de nos préoccupations.

La vie privée signifie être en mesure de mener des activités licites sans que chacun des gestes posés soient surveillés de près. Bien que nous devions nous soucier des menaces à la vie privée subtiles que présentent la collecte et la gestion modernes des renseignements, il est impératif de ne pas perdre de vue la violation flagrante de la vie privée que représente la surveillance.

La surveillance vidéo est omniprésente, dans les espaces publics et privés. Nous sommes devenus tellement conditionnés à être surveillés et enregistrés lorsque nous sommes dans une banque ou un dépanneur, lorsque nous nous déplaçons dans un aéroport ou que nous franchissons une intersection. Et maintenant, ce qui est plus alarmant, nous voyons une tendance accrue de la surveillance quand nous marchons dans les rues de nos villes.

Les personnes qui se trouvent dans un espace public peuvent raisonnablement s'attendre à être observées par d'autres. C'est une chose de s'exposer aux regards fortuits d'autrui ou même de susciter un intérêt auprès de nos concitoyens, mais s'en est une autre d'être observés de façon systématique et ininterrompue, sans motif valable, par des agents de l'État.

Nous n'en sommes toutefois pas au même point que le Royaume-Uni, où un réseau croissant de surveillance vidéo, comptant deux millions de caméras vidéo selon un rapport récent, surveille les rues, les stationnements, les quartiers et les centres commerciaux. Nous n'avons pas non plus emboîté le pas aux États-Unis, où on pratique déjà la surveillance vidéo aléatoire de rassemblements publics et où on utilise des bases de données biométriques, ce qui constitue l'équivalent électronique d'un alignement de confrontation de la police, où chacun doit participer, qu'il soit soupçonné ou non de méfaits.

Nous avons vu des systèmes de surveillance vidéo installés dans des rues publiques à Kelowna (C.-B.) – ce qui a fait l'objet d'une plainte au Commissariat – et des systèmes semblables sont prévus dans diverses autres villes canadiennes.

En outre, la technologie biométrique de reconnaissance de visage, dans les casinos en Ontario et à l'Aéroport international Pearson de Toronto, a également fait les manchettes cette année. (Dans cette dernière affaire, les reportages se sont avérés erronés; mon enquête a révélé que la GRC fait un usage raisonnable de la technologie biométrique. Le lecteur peut se reporter au compte rendu de cette affaire dans la première partie du présent rapport.)

La justification de la surveillance est toujours la même : elle accroît la sécurité et dissuade le crime. Ces raisons ne peuvent être écartées du revers de la main. Qu'il s'agisse de voler une banque ou de brûler un feu rouge, les défenseurs des droits à la vie privée ne tolèrent pas que des personnes invoquent le respect de la vie privée pour excuser les manquements délibérés aux règles et aux lois de la société.

Mais, comme quelqu'un l'a déjà dit, le seul endroit où les agents policiers ont la tâche facile, c'est dans un État policier. Nous ne pouvons laisser les préoccupations légitimes au sujet de la sécurité éclipser les préoccupations légitimes au sujet de la vie privée. Si nous mettons tout le monde dans le même bateau, si tout le monde devient un suspect dont chaque agissement doit être surveillé et peut-être enregistré, analysé et classé, juste au cas, il se peut que nous ayons fait tout ce que nous pouvons pour empêcher le crime et exercer un contrôle sur lui. Mais nous l'aurons fait au détriment du respect d'un droit de la personne fondamental.

Si l'État n'a pas raison de surveiller les citoyens respectueux des lois, le secteur privé l'a encore moins. Pourtant cette année, une entreprise de sécurité privée à Yellowknife a décidé de faire de la surveillance publique son affaire, et a braqué ses caméras vidéo sur une rue au centre-ville. Cela a suffi pour qu'une plainte

« CE QU'IL FAUT SOULIGNER INSTAMMENT DANS CETTE AFFAIRE, C'EST QU'IL N'Y A ABSOLUMENT AUCUNE PREUVE QUE LA SURVEILLANCE VIDÉO RÉDUIT DE FAIT LA CRIMINALITÉ, AU LIEU DE TOUT SIMPLEMENT LA DÉLOGER VERS D'AUTRES ENDROITS OÙ IL N'Y A PAS DE CAMÉRAS.

soit déposée aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques*, qui s'applique à toutes les activités du secteur privé dans les Territoires. J'ai indiqué mes conclusions à ce sujet dans la deuxième partie du présent rapport, et je me contenterai de dire que cette pratique contrevenait à la *Loi*. Je crois que nous pouvons tous être satisfaits d'apprendre que cette entreprise n'a pas joui de l'appui des représentants municipaux, des forces policières ou du public, et qu'elle a accepté volontiers de mettre fin à ses activités de surveillance lorsque le public s'y est opposé.

Ce qui est encore plus perturbant, c'est la situation à Kelowna, en Colombie-Britannique. La GRC, à titre de force policière municipale, a installé une caméra vidéo pour surveiller de façon continue et enregistrer tous les passants dans une rue publique. En enquêtant sur une plainte qu'avait déposée au Commissariat le Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, j'ai conclu que cette activité de collecte de renseignements personnels constituait une contravention claire à la *Loi sur la protection des renseignements personnels*.

Pourtant, la GRC poursuit sa surveillance vidéo jour et nuit, mais sans effectuer d'enregistrement continu des déplacements. Ce faisant, la GRC est techniquement conforme à la *Loi sur la protection des renseignements personnels*, où il est défini que les renseignements personnels sont des renseignements sur un individu identifiable qui sont « consignés sous une forme ou autre ».

Comme je l'ai montré clairement dans ma conclusion, je considère cette forme de surveillance vidéo des endroits publics comme une violation extrêmement grave des droits à la vie privée, même en l'absence d'un enregistrement. C'est la présence même des caméras vidéo, qu'elles enregistrent ou non à un moment donné, qui suscite le sentiment d'être observé et qui sape la vie privée. De plus, si nous permettons la prolifération des caméras vidéo, il est presque certain que l'implantation progressive de cette fonction entraînera inexorablement l'association des caméras et de la technologie biométrique. Ainsi, il se peut qu'il soit éventuellement possible d'identifier toute personne qui se trouve dans un endroit public sous surveillance continue, ou de surveiller les allées et venues et les activités d'un individu donné alors qu'il se déplace d'un endroit à l'autre.

Ce qu'il faut souligner instamment dans cette affaire, c'est qu'il n'y a absolument aucune preuve que la surveillance vidéo réduit de fait la criminalité, au lieu de tout simplement la déloger vers d'autres endroits où il n'y a pas de caméras. De fait, un porte-parole du détachement de la GRC à Kelowna, le caporal Reg Burgess, a déclaré le 19 juin 2001 au *Vancouver Sun*, que ces caméras « peuvent dans certaines circonstances prévenir le crime, mais qu'elles réussissent surtout à le déplacer ». [traduction libre]

Le journaliste de cet article du *Vancouver Sun* a poursuivi en disant : « M. Burgess a ajouté qu'en déplaçant le crime hors du centre-ville de Kelowna vers les quartiers résidentiels, la police serait alertée d'activités criminelles plus rapidement par les résidents. » [traduction libre]

Parce que mon mandat prévoit que je surveille l'application des lois sur la vie privée plutôt que l'application des lois générales, il n'est probablement pas de mon ressort de commenter la politique sur l'utilisation des caméras vidéo de la GRC en vue de déplacer la criminalité des centres-villes vers les quartiers résidentiels.

Toutefois, j'ai récemment rencontré le Commissaire de la GRC, Giulliano Zaccardelli, et j'ai tâché tant bien que mal de le convaincre de respecter les droits à la vie privée en ordonnant le retrait des caméras de surveillance à Kelowna. Dans une lettre datée du 27 novembre 2001, M. Zaccardelli m'a répondu :

> Je suis satisfait que dans le cas de Kelowna, la GRC exerce son devoir de protéger la collectivité en s'appuyant sur des préoccupations en matière de sécurité publique bien formulées. L'utilisation des caméras représentera un atout valable pour la collectivité et permettra de mettre fin aux activités criminelles et d'accroître la sécurité à cet endroit. [traduction libre]

J'ai alors demandé au Commissaire Zaccardelli de me fournir les données sur lesquelles il fonde ses conclusions, à savoir que la surveillance vidéo appuie effectivement la GRC dans son devoir de protéger la collectivité, et surtout la preuve que les caméras en opération depuis février dernier parviennent de fait à « mettre fin aux activités criminelles » et à faire de Kelowna un endroit plus sûr où vivre. Plus particulièrement, j'ai demandé au Commissaire Zaccardelli de me faire parvenir des statistiques sur le nombre d'arrestations qui découlent de l'utilisation de la caméra depuis février dernier ainsi que des statistiques comparant le taux de criminalité global à Kelowna durant les mois où la caméra était en opération avec le taux de criminalité pour la même période l'an dernier. Il ne m'a toujours pas fait parvenir ces renseignements.

Je trouve cette situation fort déplorable. On pourrait s'attendre que le Commissaire de la GRC, qui choisit de ne pas tenir compte d'une recommandation vigoureuse d'un haut fonctionnaire du Parlement dans une affaire aussi importante, fonde sa décision sur une preuve la plus contraignante qui soit, au lieu de l'appuyer sur des conjectures non corroborées ou des idées chimériques.

Ce qui est plus important, c'est qu'on pourrait s'attendre d'un agent de police du plus haut rang au Canada, c.-à-d. le dirigeant de la force policière nationale, qu'il veuille que celle-ci donne l'exemple en établissant les normes les

> « J'ai respectueusement demandé le concours des députés et des sénateurs afin de persuader le Commissaire Zaccardelli pour qu'il révise sa position relativement à cette affaire.

plus rigoureuses qui soient concernant le respect des droits à la vie privée. J'ai bon espoir que le Commissaire Zaccardelli conviendra éventuellement du bien-fondé de cette avis. S'il persiste toutefois dans sa position actuelle sur la surveillance vidéo, il donnera malheureusement un tout autre exemple, que suivront les forces policières partout au pays.

Le niveau et la qualité de la vie privée au pays risquent d'être assénés, un coup démoralisant et irréparable si nous permettons d'être surveillés et observés constamment de manière constante and ininterrompue par des caméras vidéo en prolifération qui sont sous le contrôle de la police ou d'autres agents de l'État.

C'est pourquoi, j'ai respectueusement demandé le concours des députés et des sénateurs afin de persuader le Commissaire Zaccardelli pour qu'il révise sa position relativement à cette affaire. Cette question est pour moi de la plus grande importance.

La surveillance vidéo est le moyen le plus évident par lequel nous sommes surveillés et observés en public. Mais il y en a d'autres. La technologie de repérage qui est installée dans les téléphones cellulaires permet de situer l'emplacement d'un utilisateur dans un rayon de 50 mètres. La technologie de positionnement géographique peut servir à localiser les véhicules. Les systèmes de paiement électronique utilisés sur les routes et les ponts à péage peuvent également être utilisés pour suivre le déplacement des véhicules.

Nous avons bien dépassé ce que « sortir en public » signifiait autrefois. Lorsque nous sommes en public, nous sommes *réellement* en public; il semble qu'il n'y ait rien qui soit privé.

Et ce qui accuse le problème, à mesure que la distinction entre ce qui est public et privé s'estompe, l'assaut porté contre la vie privée en public gagne les domaines que nous considérions déjà comme indiscutablement privés. Un nombre croissant de technologies d'amplification sensorielle, les capteurs chimiques et à ondes acoustiques, les dispositifs à imagerie thermique, les jumelles à infrarouge, les appareils portatifs à rayons X, permettent « d'écouler » dans les endroits publics ce qui se passe dans les endroits privés et fermés. La célèbre affaire *Kyllo* aux États-Unis, où une opération clandestine de culture de marijuana a été repérée au moyen d'un dispositif à imagerie thermique qui a capté la transmission thermique à l'extérieur de la maison, montre à quel point la distinction entre ce qui est public et privé est floue.

De nouveau, les défenseurs des droits à la vie privée ne plaident pas la cause de la criminalité. Ils reconnaissent les bonnes intentions de ceux qui veulent recourir à la surveillance pour accroître la sécurité. Mais notre société peut atteindre ses objectifs légitimes en matière de sécurité et de prévention de la criminalité sans toutefois se défaire des droits à la vie privée et des libertés civiles fondamentales qui en découlent. Ces technologies intrusives dans la vie privée doivent être confinées à des situations limitées et particulières, où la menace à la sécurité publique est matérielle, importante et imminente, et elles doivent être visées par une autorisation judiciaire préalable, autrement dit, être assorties de mandats.

Même l'accroissement extraordinaire de l'utilisation généralisée de la surveillance exercée sur notre personne publique par les agents de l'État, n'est rien comparativement à l'explosion de la surveillance des employés à la fois en milieu de travail et hors de celui-ci. Il s'agit d'une question qui m'inquiète de plus en plus.

Comme je l'ai mentionné lors d'une conférence à Toronto en avril dernier, la vie privée en milieu de travail est une question qui a pris de plus en plus d'importance, car la protection implicite de la vie privée n'est plus suffisante. En outre, les droits à la vie privée en milieu de travail ne sont pas bien définis, car jusqu'à présent, il n'était pas nécessaire qu'ils le soient.

Les gestionnaires ont toujours voulu assurer le rendement et prévenir la redevabilité. Même avant que Henry Ford et Frederick Taylor n'aient mis en place la chaîne de montage et la « gestion scientifique », les gestionnaires surveillaient, mesuraient et exerçaient un contrôle sur les travailleurs.

Mais pendant longtemps, la technologie imposait une limite bénigne à tout cela. Les travailleurs pouvaient maintenir leur vie privée lorsqu'ils étaient au travail, au même titre qu'ils assuraient la confidentialité du contenu de leurs tiroirs de bureau, casiers et de leurs effets personnels, du simple fait que la surveillance et l'enregistrement pouvaient aisément être surchargés de renseignements.

Cette limite bénigne a commencé à disparaître lorsque l'usage des ordinateurs s'est répandu. L'illusion d'une sécurité et d'un contrôle parfaits est pratiquement réalisable en milieu de travail, en raison de la technologie qui permet aux gestionnaires de surveiller tous les déplacements et d'analyser tout ce qui est enregistré.

« LES EMPLOYÉS NE RENONCENT PAS À LEUR DROIT FONDAMENTAL À LA VIE PRIVÉE LORSQU'ILS SIGNENT UN CONTRAT DE TRAVAIL.

La notion que les employés ont des droits à la vie privée en milieu de travail est inacceptable pour certains, parce que ceux-ci sont à l'emploi et dans les locaux de l'employeur, utilisant son matériel. Je ne suis pas d'accord. Les employés ne renoncent pas à leur droit fondamental à la vie privée lorsqu'ils signent un contrat de travail. Et cela peut en surprendre certains qu'un nombre considérable de juges et d'arbitres partagent mon avis.

Néanmoins, nous avons été témoin d'un extraordinaire accroissement de la surveillance en milieu de travail. Cela est surtout apparent aux États-Unis, où il n'y a pas de loi en vigueur pour assurer la protection de la vie privée des employés, En janvier 2001, l'American Management Association a sondé 1 627 moyennes et grandes entreprises et a révélé que plus de 75 % d'entre elles font un enregistrement vidéo de leurs employés ou surveillent leur courrier électronique, leur utilisation d'Internet, leurs conversations téléphoniques ou leurs fichiers informatiques. Cela représente une augmentation de près de 10 % comparativement aux résultats d'un sondage semblable mené l'an dernier.

Il n'y a pas d'études comparables de l'ampleur de la surveillance des employés au Canada, mais on croit que la situation au pays reflète celle aux États-Unis. Il se peut que cette hypothèse soit erronée, en partie parce qu'on ne comprend pas bien les différences qui existent entre les lois canadiennes et américaines.

Il arrive fréquemment qu'on ne soit pas au fait des particularités des lois au Canada. À titre d'exemple, les employeurs invoquent souvent leur responsabilité potentielle à l'égard du harcèlement en milieu de travail pour justifier une surveillance, surtout d'Internet et du courrier électronique. Cela reflète la doctrine juridique américaine, et non celle en vigueur au Canada. Au pays, la législation antidiscrimination reconnaît seulement une responsabilité à l'employeur lorsque celui-ci n'a pas pris de mesures raisonnables pour prévenir le harcèlement. Mais cela ne veut pas dire pour autant qu'il faut employer la surveillance électronique de façon généralisée en milieu de travail. Il faut plutôt adopter une politique antiharcèlement fondée, assurer la formation des employés, mettre en place des procédures antiharcèlement convenables (comme l'embauche d'un coordonnateur des initiatives antiharcèlement et un processus de plaintes confidentiel), et réagir rapidement et efficacement en l'occurrence de harcèlement ou lorsqu'on a de bonnes raisons de croire qu'il se produit.

> La surveillance électronique ne doit jamais se substituer aux pratiques de gestion et de supervision saines.

Une autre excuse qu'on avance parfois concernant la surveillance électronique généralisée est la « possibilité » de l'utilisation d'Internet qui représente une perte de temps et le mésusage du matériel de l'employeur. Je ne crois pas qu'on doive surveiller les employés pour prévenir des pertes de temps potentielles, pas plus que nous devons surveiller les citoyens respectueux des lois pour éviter la possibilité que l'un d'eux commette un crime. Les soupçons raisonnables de fautes doivent être la seule justification de la surveillance en milieu de travail. La surveillance électronique ne doit jamais se substituer aux pratiques de gestion et de supervision saines. Si la seule façon qu'a un employeur pour savoir si les employés travaillent, c'est de les surveiller avec des moyens électroniques, alors il y a quelque chose qui cloche avec les pratiques de gestion qu'il a adoptées.

La Loi sur la protection des renseignements personnels et les documents électroniques limite la collecte, l'utilisation et la communication de renseignements aux seules « fins qu'une personne raisonnable estimerait acceptables dans les circonstances ». Il s'agit d'une importante restriction de la surveillance en milieu de travail. Parce que la *Loi*, ou une loi provinciale similaire, aura bientôt force exécutoire pour les employeurs partout au pays, ceux-ci auraient intérêt à en prendre connaissance.

J'ai mentionné ci-dessus les implications sur la vie privée qui découlent des pressions exercées pour assurer la transparence au sein des gouvernements et l'accès aux renseignements qu'ils détiennent. Cette question est arrivée au point critique cette année car diverses parties ont tenté d'avoir accès à l'emploi du temps du premier ministre, et ils étaient appuyés dans leur tentative par le Commissaire à l'information.

Que les valeurs de transparence et d'accès à l'information ont pu être déformées à ce point et constituer une attaque à la vie privée – les emplois du temps sont de par leur nature même privés – a été une bien pénible découverte pour moi. Je n'ai jamais cru que je m'opposerais à une demande d'accès à l'information. En tant qu'ancien journaliste, je suis sensibilisé au plus haut point à l'importance de la transparence au sein des gouvernements. Et en tant que citoyen activement engagé, j'ai vu comment il est possible d'accroître la responsabilité en rendant facilement accessible l'information.

Mais cette bonne intention ne peut ni tout invalider ni justifier la violation du droit à la vie privée individuelle. De nouveau, il faut défendre la vie privée dans toute son importance sociétale, en tant que droit fondamental, de façon que celle-ci ne soit pas perçue comme quelque chose à échanger chaque fois qu'on y voit un obstacle à un objectif valable.

Heureusement, je ne suis pas le seul à m'inquiéter à ce sujet. Les tribunaux ont été très clairs : la transparence du gouvernement n'empêche pas la protection des droits humains fondamentaux. L'accès est un droit administratif qui peut rehausser la démocratie. Et la vie privée est un droit humain fondamental qui est de l'essence même de la démocratie.

Une autre importante question est l'initiative Gouvernement en direct. La transition à une interface électronique homogène entre les citoyens et les divers paliers de gouvernement peut s'avérer bénéfique, améliorant la prestation des programmes ainsi que l'efficacité et l'accessibilité des gouvernements. Tous les Canadiens et Canadiennes ont une histoire à raconter au sujet de la confusion concernant le ministère ou le palier d'administration chargé d'un service donné auquel faire appel. Et bon nombre de Canadiens et Canadiennes connaissent des histoires, qu'elles soient vraies ou anecdotiques, au sujet des difficultés éprouvées lorsqu'on tente d'obtenir des renseignements du gouvernement.

Mais les distinctions entre les organismes et les programmes, au sein du gouvernement ou dans l'ensemble des paliers de gouvernement, présentent des obstacles à la collecte de renseignements personnels. Le gouvernement en tant qu'organisme unique et centralisé rend possible la fusion des bases de données, qui renferment des renseignements sur les interactions des particuliers avec le gouvernement. Ces renseignements ont été recueillis à des fins particulières. Lorsque les renseignements sont conservés dans des bases de données distinctes pour des usages particuliers, ils sont compartimentés.

Lorsque les bases de données sont fusionnées, une personne qui a besoin d'un seul élément d'information peut avoir accès à bon nombre de renseignements. Et tout renseignement peut être combiné seulement à d'autres et révéler de nouveaux renseignements, rendant possible l'établissement de profils détaillés sur les individus, le suivi de leurs activités et de leur interaction avec le gouvernement. Combiné à tout cela est l'attribution à chaque Canadien et Canadienne d'un mécanisme d'authentification, d'identification et d'accès – que le gouvernement désigne comme la « cyberidentité ». Nous pourrions bientôt nous trouver dans une société de surveillance et ne plus avoir droit à la solitude.

> La vie privée doit être intégrée dès le départ à l'initiative Gouvernement en direct.

De plus, la prestation de services ou le versement de prestations par voie électronique demandera la participation du secteur privé. Les fournisseurs du secteur privé, à titre d'éléments du système de prestation du gouvernement, pourraient devenir des dépositaires de vastes bases de données sur les Canadiens et Canadiennes. Cela est sujet d'inquiétude, compte tenu de la protection restreinte de la vie privée dans le secteur privé, même avec la nouvelle *Loi* qui le vise.

Je me suis adressé à de nombreux auditoires cette année à ce sujet, et j'ai entrepris des consultations continues avec le gouvernement du Canada. Mon message est pourtant simple : la vie privée doit être intégrée dès le départ à l'initiative Gouvernement en direct. Cela comprend la tenue d'évaluations de l'incidence sur la vie privée et la consultation des organismes de protection de la vie privée à l'étape de la conception, et pas en bout de ligne, lorsque les difficultés liées à la vie privée sont déjà ancrées.

Encore une fois, je ne remets pas en question les motifs des responsables de ces initiatives. Il ne fait aucun doute, à mon esprit, que leurs intentions sont les meilleures. L'efficience est une aspiration louable. Mais, comme je l'ai maintes fois répété, il faut comprendre à juste titre l'efficience en tant que rapport entre les moyens et les fins, de façon à choisir les meilleurs moyens pour atteindre des fins précises. Ce qui est critique, c'est la façon de définir ces objectifs. Pour les gouvernements et la société, ces objectifs doivent comprendre la préservation et la protection de la vie privée.

Plus tôt, j'ai brièvement abordé la question des renseignements personnels sur la santé. Il est bien difficile de faire valoir à quel point cette question est importante.

Les gouvernements aux paliers provincial et fédéral ont l'intention d'accroître les activités de collecte et de partage des renseignements médicaux personnels et d'élaborer un système exhaustif de renseignements sur la santé. Leur intention est louable – assurer des soins normalisés et cohérents dans tout le pays, se renseigner sur les causes des maladies, et déterminer qui utilise à bon ou à mauvais escient le système et pourquoi.

Mais, en bout de ligne, le dernier examen médical d'une personne peut potentiellement en viser des milliers d'autres. Et parce que l'état du système de santé représente une préoccupation majeure, les questions touchant la vie privée pourraient être mises de côté, ou du moins n'être abordées que sommairement dans le cadre des discussions.

La perte de contrôle sur les renseignements personnels sur la santé peut comporter des conséquences dévastatrices. Et la crainte de perdre ce contrôle peut inciter certaines personnes à ne pas recourir aux services médicaux. La possibilité d'évaluations psychiatriques détaillées tombant entre les mains d'un administrateur d'assurance ou d'un employeur, par exemple, peut suffire à dissuader des personnes à obtenir des soins. Ou elles peuvent ne pas communiquer des renseignements vitaux à leur médecin, ce qui minerait l'efficacité des traitements et, en fin de compte, gaspillerait les ressources du système de soins de santé.

Dans un récent sondage aux États-Unis, près de 87 % des médecins ont indiqué qu'un patient leur avait demandé de ne pas ajouter certains renseignements à leur dossier. Près de 78 % ont dit qu'ils n'avaient pas versé ces renseignements au dossier, en raison de préoccupations relatives à la vie privée. Il faut se demander si des attitudes semblables sont courantes au Canada.

Concernant un patient donné, les renseignements sur sa santé sont fondamentalement personnels et délicats. Il faut leur assurer le niveau de protection le plus élevé pour que ceux-ci ne soient jamais utilisés au détriment de l'individu auquel ils se rapportent.

Je suis très inquiet au sujet de la sécurité des renseignements médicaux personnels de nature délicate. Le stockage électronique des dossiers médicaux peut non seulement accroître les violations isolées à la vie privée, mais aussi les violations en règle. Nous avons tous entendu parler de communications involontaires de renseignements personnels sur la santé et des manquements à la sécurité sur Internet.

Qu'on pense à l'exemple récent de la communication non autorisée par Eli Lilly de 700 adresses électroniques de personnes qui prenaient l'antidépresseur Prozac. Eli Lilly avait offert aux patients, qui prenaient ce médicament, un service de rappel par courrier électronique. La violation de la vie privée s'est produite lorsqu'un message électronique transmis à la fin de juin et annonçant la fin du programme, comprenait les adresses électroniques des personnes qui s'étaient inscrites au service. Cette seule action a suscité beaucoup de publicité négative pour l'entreprise et a alimenté le débat aux États-Unis au sujet de la difficulté d'assurer la protection des dossiers des patients qui sont archivés électroniquement.

Nous avons également pris connaissance de cas de pirates qui ont eu accès à des dossiers médicaux. En décembre 2000, le *Washington Post* a signalé qu'un pirate hollandais s'était introduit dans le système des dossiers de

LA VIE PRIVÉE N'EST PAS UNE OPTION, PAS PLUS QU'UNE FRIVOLITÉ. C'EST UN DROIT FONDAMENTAL.

patients à l'University of Washington Medical Center, de Seattle. Le pirate avait téléchargé plusieurs milliers de dossiers qui renfermaient le nom, la condition médicale, l'adresse domiciliaire et le numéro de sécurité sociale des patients. Au pays, le *Vancouver Sun* indiquait, en août, que cinq pharmaciens de la Colombie-Britannique avaient récemment été frappés de sanctions disciplinaires et d'amendes par le Collège des pharmaciens de la province pour avoir indûment pris connaissance des dossiers sur les médicaments de collègues, de parents, d'amis ou de connaissances.

Sommes-nous prêts, en tant que société, à faire face aux manquements à la vie privée et à la sécurité qui peuvent se réaliser? Sans doute, au bas mot, nous devrions demander aux patients s'ils veulent que leurs dossiers médicaux au complet soient stockés sur des supports électroniques. Nous reconnaissons que les dossiers électroniques des patients représentent une autre occasion d'améliorer la qualité des soins. Mais nous devons en même temps reconnaître que ces dossiers peuvent susciter des difficultés liées à la vie privée des patients et à la confidentialité de leurs renseignements. On ne peut donner suite à cette possibilité si nous ne pouvons relever les défis.

En effet, ce seul fait – que les possibilités d'avenir ne peuvent être réalisées de façon satisfaisante sans relever le défi que présente la protection de la vie privée – concerne toutes les questions avec lesquelles j'ai affaire et que j'ai abordées dans le présent compte rendu.

La vie privée n'est pas une option, pas plus qu'une frivolité. C'est un droit fondamental. La nécessité de respecter ce droit tient à l'essentiel de nos espoirs de progrès en tant que société et qu'individus, car tout progrès important vise avant tout à accroître notre qualité de vie. Et nous ne devons jamais nous bercer d'illusions que nous pouvons réaliser une telle amélioration si nous l'envisageons, dans quelque domaine que ce soit, en sacrifiant étourdiment le droit à la vie privée, qui est essentiel à notre liberté et à notre dignité.

Il nous faut combattre cette illusion là où elle se présente et ne pas faire ce sacrifice lorsqu'on tente de nous l'imposer, voilà les visées propres au Commissariat. Dans les parties suivantes du rapport, je rendrai compte des façons dont nous nous sommes acquittés de nos responsabilités.

Première partie
Rapport concernant la *Loi sur la protection des renseignements personnels*

Introduction

La *Loi sur la protection des renseignements personnels* assure la protection de la vie privée des individus pour ce qui est des renseignements personnels détenus par les institutions fédérales.

La *Loi*, qui est entrée en vigueur en 1983, régit les moyens pris par les institutions fédérales pour recueillir, utiliser, communiquer et retirer des renseignements personnels, et accorde aux individus le droit d'accéder à leurs renseignements personnels et de demander des corrections au besoin. La *Loi* établit également mes devoirs et responsabilités ainsi que mon mandat.

À titre de Commissaire à la protection de la vie privée, je reçois des plaintes d'individus qui croient que leurs droits aux termes de la *Loi* ont été violés et je fais enquête sur ces plaintes. Je peux également prendre l'initiative d'une plainte et faire enquête moi même concernant toute situation pour laquelle j'ai des motifs raisonnables de croire que la *Loi* a été violée.

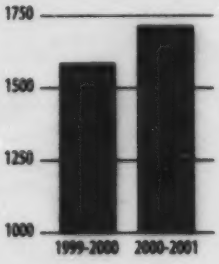
Je suis d'abord avant tout un ombudsman, et je tâche dans la mesure du possible de régler les plaintes par la médiation et la négociation. Mais je possède également de vastes pouvoirs d'enquête qui me sont conférés par la *Loi*. En tant que Commissaire à la protection de la vie privée, je peux contraindre des témoins à comparaître et à témoigner, par exemple, et je peux pénétrer dans des locaux afin d'obtenir des documents et tenir des entrevues.

L'entrave aux enquêtes est une infraction à la *Loi*. Je ne peux toutefois pas contraindre à la conformité avec la *Loi sur la protection des renseignements personnels*, mais je peux recommander des changements à la manière dont les institutions fédérales traitent les renseignements personnels et qui découlent des conclusions de mes enquêtes.

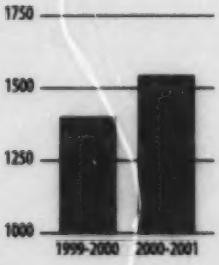
Suivant mon mandat en tant que Commissaire à la protection de la vie privée, je peux également effectuer des vérifications périodiques dans les institutions fédérales afin de déterminer leur niveau de conformité avec la *Loi sur la protection des renseignements personnels* et, sur la base de mes conclusions d'enquête, je peux recommander des changements.

Aux termes de la *Loi*, je suis tenu de déposer un rapport annuel au Parlement sur les activités de l'exercice antérieur du Commissariat. Le présent rapport vise la période du 1er avril 2000 au 31 mars 2001.

Nombre de plaintes reçues
1er avril 2000 - 31 mars 2001



Enquêtes sur les plaintes terminées
1er avril 2000 - 31 mars 2001



Enquêtes

La Direction des enquêtes et demandes de renseignements mène des enquêtes sur les plaintes déposées par des individus aux termes de l'article 29 de la *Loi sur la protection des renseignements personnels* (et aux termes de l'article 11 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, dont il sera question ci-après dans le présent rapport).

Par le biais de ces enquêtes, je détermine si les droits à la vie privée des individus ont été violés ou si ces derniers ont pu avoir accès de façon convenable à leurs renseignements personnels. Lorsque les droits à la vie privée d'individus ont été violés, je leur offre des moyens de recours et j'envisage des façons pour empêcher que les violations se reproduisent.

Je suis également autorisé aux termes de la *Loi* à faire prêter serment, à recevoir les éléments de preuve et à entrer dans des locaux. Je peux également examiner ou me faire remettre des copies de documents trouvés dans n'importe quel local.

Jusqu'à présent, toutes les plaintes déposées en vertu de la *Loi sur la protection des renseignements personnels* ont été réglées sans que nous ayons dû invoquer ces pouvoirs d'enquête officiels, parce qu'on a fait preuve de collaboration volontaire lors des enquêtes.

La Direction a également répondu à des milliers de demandes de renseignements du grand public, qui communique avec le Commissariat pour demander des conseils et de l'aide sur toutes sortes de questions touchant la vie privée.

Plaintes en vertu de la *Loi sur la protection des renseignements personnels*

Du 1er avril 2000 au 31 mars 2001, nous avons reçu au total 1 713 plaintes en vertu de la *Loi sur la protection des renseignements personnels*,

ce qui représente une augmentation de près de 10 % par rapport à l'an dernier. Les genres de plaintes que nous avons reçues concordent également à la tendance établie, c.-à-d. 60 % d'entre elles concernaient soit l'accès refusé aux renseignements personnels soit des questions touchant la collecte, l'utilisation, la communication et le retrait des renseignements personnels, et les 40 % restantes visaient le non-respect des échéances par des organismes fédéraux, qui n'avaient pas donné réponse à une demande de communication de renseignements personnels dans le délai de 30 jours établi dans la *Loi*.

Mon personnel a mené à terme 1 542 enquêtes, autre augmentation de 10 % depuis l'an dernier. Parmi les affaires réglées, 339 touchaient des questions de collecte, d'utilisation, de communication ou de retrait, tandis que 630 se rapportaient à l'accès et 573, aux délais. Les décisions relativement aux plaintes ont été rendues comme suit :

Non fondées :	421
Fondées :	553
Fondées et résolues :	82
Résolues :	44
Résolues en cours d'enquête :	321
Abandonnées :	121

Les plaintes déposées au sujet de ministères qui ne répondent pas aux demandes d'accès dans les délais impartis sont toujours troublantes, car justice différée est justice refusée, et les délais fixés dans la *Loi* l'ont été pour de bonnes raisons.

Plusieurs institutions du gouvernement fédéral se distinguent par le fait qu'il leur arrive trop souvent de ne pas répondre dans les délais prescrits aux demandes d'accès aux renseignements personnels que leur adressent des individus. Il s'agit du Service correctionnel du Canada, du ministère de la Défense nationale, de l'Agence des douanes et du revenu du Canada et de Développement des ressources humaines Canada.

Il m'apparaît de la plus haute importance que tous les ministères et organismes de l'État respectent rigoureusement les délais fixés par la *Loi sur la protection des renseignements personnels*. Le respect des droits que la loi confère aux Canadiens et Canadiennes est obligatoire, et non pas discrétionnaire. Aucune entité du gouvernement du Canada n'a d'excuse pour violer une loi du Canada, et j'entends bien continuer d'insister sur ce point.

Service correctionnel du Canada

À l'automne 2000, compte tenu du nombre de plaintes de non-respect des délais dont a fait l'objet le Service correctionnel du Canada, j'ai chargé mon personnel d'examiner la question avec les cadres supérieurs du SCC.

En février 2001, la Commissaire du Service correctionnel a convenu de mettre en œuvre certaines mesures pour éliminer l'arriéré de demandes dans son Ministère.

Ces mesures ont entraîné une amélioration du traitement des plaintes d'accès au Service correctionnel. En mars 2001, le Ministère avait en cours de traitement 1 684 demandes actives d'accès, dont il avait respecté le délai prescrit de réponse dans seulement environ 20 % des cas. Le 31 août 2001, après une injection de personnel et d'heures supplémentaires, le Ministère a réussi à ramener à 501 le nombre de demandes actives. Près de 60 % de ces demandes ont eu une réponse dans le délai prescrit, et 30 % étaient en retard de 30 jours ou moins.

Certes, il s'agit-là d'une amélioration, et, le 1er juillet, j'ai félicité la Commissaire du Service correctionnel pour la réalisation de son ministère. Le Service correctionnel continue de s'employer à réduire le nombre de demandes en instance et d'abréger son temps de réponse. Je m'en réjouis, mais cela ne me rend pas euphorique. Rien de moins ne serait acceptable.

Ministère de la Défense nationale

Le personnel du Commissariat a commencé à examiner la question des délais de réponse avec les fonctionnaires du ministère de la Défense nationale à la fin de 1999. À l'époque, le Ministère avait environ 2 100 demandes d'accès en instance. La grande majorité n'avaient pas été traitées dans le délai prescrit. Sur les instances de mes fonctionnaires, le Ministère a convenu de prendre des mesures comme l'embauche de personnel supplémentaire, le travail en heures supplémentaires et la restructuration de ses procédures et de son organisation internes.

Ces efforts ont porté fruit. En novembre 2001, le Ministère avait ramené à 279 le nombre de demandes d'accès en instance. Un peu moins de la moitié, soit 136, n'étaient pas traitées dans les délais prescrits.

Ces chiffres traduisent une amélioration, mais la situation demeure inacceptable. Je reconnais que, pour l'essentiel, les demandes ont trait à de gros dossiers de renseignements concernant des choses comme les enquêtes policières, les commissions d'enquête, ou les plaintes de harcèlement. Le traitement de ces plaintes est difficile. Mais cela doit être un défi, et non pas une excuse.

Agence des douanes et du revenu du Canada

L'Agence a eu d'importantes difficultés à respecter les délais de réponse aux demandes d'accès. Le personnel du Commissariat s'est réuni avec les représentants de l'Agence au début de 2000, tout comme il l'avait fait avec le ministère de la Défense nationale. L'Agence, tout comme la Défense nationale, a accepté de prendre des mesures, comme la réorganisation et l'embauche de nouveau personnel, pour améliorer la situation.

Dans les deux exercices qui ont précédé l'exercice en cours, le Commissariat a reçu 81 plaintes de non-respect des délais la première année, et 127 l'année suivante. La quasi-totalité (95 % la première année, 99 % l'année suivante) ont été jugées fondées.

Pendant l'exercice en cours, le Commissariat n'a reçu que 61 plaintes de non-respect des délais, dont 51 étaient fondées.

Bien que meilleurs que ceux des deux années précédentes, ces chiffres demeurent élevés. Encore une fois, les retards sont probablement le reflet de la complexité des plaintes au sujet des renseignements personnels des dossiers d'impôt, mais il reste des améliorations à apporter.

Développement des ressources humaines Canada

Nous avons reçu 80 plaintes contre Développement des ressources humaines Canada au sujet du non-respect des délais. Près de 60 %, c'est-à-dire 47, concernaient l'accès aux renseignements personnels du Fichier longitudinal sur la main-d'œuvre, le « superfichier » sur les Canadiens et Canadiennes qui a été démantelé l'an dernier à cause de problèmes de protection des renseignements personnels. Il s'agissait d'une situation exceptionnelle, compte tenu de toute l'attention que le dossier a retenue dans les médias et au Parlement, et du grand volume de demandes d'accès que le Ministère a dû traiter. Si l'on fait abstraction de ces circonstances exceptionnelles, il ne nous reste 33 plaintes au sujet des retards de réponse aux demandes d'accès. Ce nombre est encore trop élevé. Mais, compte tenu du nombre de demandes que le Ministère reçoit chaque année, et compte tenu de la taille de ce ministère, le nombre est assez faible pour permettre de croire qu'il suffirait d'un peu de réorganisation et de travail supplémentaire pour l'éliminer. Le Ministère doit s'y employer.

Le Commissariat continuera de surveiller les questions relatives aux délais et mettra de la pression pour qu'il y ait des améliorations continues.

Définitions aux termes de la *Loi sur la protection des renseignements personnels*

Non fondée : Lorsqu'une plainte est jugée non fondée, cela signifie que l'enquête n'a relevé aucun élément de preuve qui me porte à conclure que l'institution fédérale a violé les droits d'un plaignant aux termes de la *Loi sur la protection des renseignements personnels.*

Fondée : Lorsqu'une plainte est jugée fondée, cela signifie que l'institution fédérale n'a pas respecté les droits d'un individu en vertu de la *Loi sur la protection des renseignements personnels.* Ce serait également ma conclusion dans une situation où l'institution fédérale refuse d'accorder l'accès à des renseignements personnels malgré ma recommandation que ceux-ci soient communiqués. En pareil cas, la prochaine étape consiste à demander un recours en révision à la Cour fédérale du Canada.

Fondée et résolue : Je conclus qu'une plainte est fondée et réglée lorsque les allégations sont corroborées par l'enquête et que l'institution fédérale a accepté volontairement de prendre des mesures correctives pour remédier à la situation.

Résolue : Il s'agit d'une conclusion officielle qui reflète mon rôle d'ombudsman. Cette conclusion est réservée aux plaintes pour lesquelles une conclusion « fondée » serait trop sévère dans les cas de mauvaise communication ou de malentendu. Cela signifie que le Commissariat, après avoir mené une enquête complète et minutieuse, a permis de négocier une solution qui satisfait toutes les parties.

Résolue en cours d'enquête : Il ne s'agit pas d'une conclusion officielle, mais d'une façon acceptable de régler une plainte. Une fois que l'enquête est terminée, le plaignant est satisfait des efforts déployés par le Commissariat et il consent à laisser tomber l'affaire.

Le plaignant retient toutefois le droit de demander qu'une conclusion officielle soit rendue. Le cas échéant, l'enquêteur rouvre le dossier et dépose un rapport officiel. Je dois alors faire rapport sur les conclusions dans une lettre au plaignant.

Abandonnée : Il s'agit d'une enquête qui est terminée avant que toutes les allégations soient pleinement examinées. Une affaire peut être *abandonnée* pour un nombre de raisons, par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire ou il est impossible de lui demander de fournir des renseignements supplémentaires, qui sont essentiels pour en arriver à une conclusion. Je ne dépose pas de conclusion officielle lorsqu'une plainte est abandonnée.

Sommaire de cas choisis en vertu de la *Loi sur la protection des renseignements personnels*

Des renseignements personnels trouvés dans un conteneur à ordures au MDN

Dans cette affaire, des dossiers remplis de renseignements personnels ont été trouvés dans un conteneur à ordures à l'extérieur d'un manège militaire. Les dossiers renfermaient des renseignements personnels sur des douzaines d'employés du ministère de la Défense nationale (MDN), y compris leurs nom, adresse et numéro de téléphone personnels, date de naissance, renseignements médicaux et dentaires, des formulaires de vérification de sécurité, des antécédents professionnels, des formulaires d'avis au plus proche parent, des évaluations du rendement, et bien d'autres encore.

Ces renseignements, s'ils avaient été communiqués, auraient pu causer de sérieux préjudices et assurément un embarras personnel et professionnel considérable.

La personne qui a trouvé les dossiers, un réserviste, a signalé la découverte aux officiers supérieurs, mais aucune mesure n'a été prise. Il a été capable d'extraire du conteneur ce qu'il a décrit comme un petit pourcentage des dossiers avant que le conteneur ne soit déversé au dépotoir local comme d'habitude. Il a transmis les dossiers au Commissariat et a déposé une plainte, alléguant que ses renseignements personnels avaient été retirés de façon indue.

Mon enquête a permis d'établir qu'un bureau devait être réinstallé à un autre étage et, pour préparer le déménagement, on avait ordonné de procéder au retrait de tout ce qui n'était pas nécessaire dans le nouvel emplacement. Le bureau tenait des dossiers parallèles ou « en double » à l'extérieur de la pièce où les dossiers officiels du MDN étaient conservés. Certains des renseignements dans ces dossiers parallèles étaient des doubles de dossiers officiels, tandis que d'autres ne l'étaient pas. Ces dossiers étaient placés dans des chemises ordinaires, qui ne portaient pas le logo du Ministère. Comme ils ne semblaient pas être importants de l'extérieur, personne n'a pensé à en examiner le contenu, et ils ont tout simplement été jetés aux ordures.

Un nombre de dossiers officiels du MDN, qui comprenaient des rapports d'étape sur des candidats renfermant des renseignements personnels détaillés, se trouvaient avec ces dossiers ordinaires.

Les fonctionnaires du MDN ont réagi rapidement, assurant au Commissariat qu'ils prendraient des mesures pour que cela ne se reproduise plus. Le MDN a également accepté de verser les renseignements trouvés dans les dossiers récupérés aux dossiers officiels du Ministère.

Bien que l'usage de « dossiers en double » ne contrevienne pas à la *Loi sur la protection des renseignements personnels*, cette pratique m'inquiète beaucoup. Maintes fois le Commissariat a trouvé des renseignements personnels conservés dans de tels dossiers à de nombreux ministères fédéraux. Il arrive souvent que les renseignements qu'ils renferment ne sont pas communiqués aux individus qui demandent accès en vertu de la *Loi sur la protection des renseignements personnels*, car ceux-ci ne sont pas conservés dans les « dossiers officiels ».

Une question qui a été soulevée au cours de l'enquête a porté sur les lignes directrices relatives au retrait de renseignements personnels du Conseil du Trésor du Canada.

Ces lignes directrices décrivent trois niveaux de renseignements personnels. Le niveau supérieur comprend les renseignements personnels qui, s'ils étaient compromis, « entraîneraient un préjudice extrêmement grave ». Le niveau intermédiaire entraînerait « un préjudice sérieux » si les renseignements étaient compromis. Selon les lignes directrices, il est recommandé de déchiqueter les renseignements personnels de ces niveaux.

Le niveau inférieur comprend les renseignements personnels de nature « peu délicate » qui, s'ils étaient compromis, « causeraient un préjudice ».

Conformément aux lignes directrices, les documents renfermant des renseignements personnels peuvent être déchirés en deux et jetés dans les conteneurs à ordures ordinaires.

Je m'oppose vigoureusement à ces lignes directrices ainsi qu'à leurs dispositions cavalières visant le retrait des renseignements qui, tel qu'il y est reconnu, pourrait causer un préjudice. En outre, je ne reconnais pas la validité de la distinction entre un « préjudice » et un « préjudice grave ». Lorsqu'il est question de vie privée, tout préjudice est grave. La seule façon acceptable de détruire n'importe quel genre de renseignements personnels est de les déchiqueter.

Le MDN n'est pas la seule institution fédérale à suivre ces lignes directrices. Mes discussions avec les agents de sécurité du MDN sur cette affaire se poursuivent.

Des renseignements personnels détruits de façon prématurée à DRHC

Mon enquête suivant cette plainte m'a permis de conclure que Développement des ressources humaines Canada (DRHC) avait violé à la fois de la *Loi sur la protection des renseignements personnels* et son propre Guide sur les politiques.

Un prestataire d'assurance-emploi s'est plaint au Commissariat que sa capacité d'obtenir tous les renseignements dont il avait besoin pour interjeter un appel avait été entravée par

la destruction par DRHC d'une audiocassette de l'audience initiale relative à son cas devant le Conseil arbitral.

Le Guide sur les politiques de DRHC précise que les cassettes doivent être « conservées pendant une période maximale d'un an ou jusqu'à ce que le cas ait été entendu par (le bureau de) l'arbitre, la Cour fédérale ou la Cour suprême, ainsi qu'en prévision d'une nouvelle enquête par le Conseil arbitral, les arbitres, etc ». Le plaignant avait obtenu deux audiences auprès du Conseil arbitral et avait comparu devant trois arbitres (juges à la Cour fédérale), mais n'avait pas épuisé tous les niveaux d'appel et était prêt à présenter son cas à la Cour fédérale et à la Cour suprême. Ainsi, conformément à la politique de DRHC, l'audiocassette n'aurait pas dû être détruite.

De plus, le *Règlement sur la protection des renseignements personnels* exige des institutions fédérales qu'elles conservent les renseignements personnels utilisés pour prendre une décision administrative pendant une période d'au moins deux ans, pour que l'individu concerné puisse y avoir accès.

Par suite de mon enquête, DRHC a convenu de modifier son Guide sur les politiques, de façon à prévoir une période de conservation de deux ans des audiocassettes utilisées lors d'audiences devant le Conseil arbitral. Il a également modifié le Guide pour renseigner le personnel sur l'obligation de conserver les renseignements personnels pendant une période de deux ans après les audiences à tous les niveaux juridictionnels, y compris la Cour suprême. Une instruction à cet effet a été envoyée au personnel et la Division des appels a fait paraître une modification du Guide sur les politiques.

Statistique Canada : préoccupations concernant la publication de renseignements sur certains groupes

Cette plainte a soulevé l'intéressante question de la « protection des renseignements collectifs », et dénote la nécessité de faire preuve de prudence au moment de publier des renseignements sur des groupes identifiables. Bien que les communications de ce genre puissent ne pas permettre d'identifier un individu en particulier, elles comportent toutefois une incidence sur la vie privée car les renseignements sur le groupe peuvent porter atteinte à la vie privée de chaque individu dans le groupe.

Dans ce cas particulier, un homme qui avait été sollicité plusieurs fois au téléphone par des sociétés de courtage a déposé une plainte à l'endroit de Statistique Canada, alléguant que Statistique Canada avait communiqué un nombre important de ses renseignements personnels, obtenus auprès de l'Agence des douanes et du revenu du Canada, pour permettre à une société de recherche de déterminer son revenu annuel.

L'enquête a révélé que les renseignements vendus par Statistique Canada à la société de recherche avaient de fait été tirés du Recensement de 1991 et non des dossiers d'impôt sur le revenu, comme l'avait allégué le plaignant. Et même si les renseignements se rapportaient à une région géographique donnée, ils n'étaient pas organisés selon le code postal, comme l'avait cru le plaignant. En outre, les renseignements ne concernaient pas des individus identifiables ou n'étaient pas de nature personnelle, tels que définis dans la *Loi sur la protection des renseignements personnels*.

Bref, Statistique Canada n'a pas contrevenu à la *Loi sur la protection des renseignements personnels*. Toutefois, la plainte a soulevé une importante question touchant la vie privée des membres de groupes identifiables.

Les produits et services de recensement, même ceux fondés sur des renseignements recueillis auprès d'un échantillon aléatoire de la population de 20 %, peuvent fournir des données suffisamment exactes et détaillées sur les caractéristiques d'une population dans une région géographique donnée. Les sociétés de recherche peuvent assembler des renseignements obtenus de Statistique Canada, ce qu'elles font, sur la base des renseignements tirés d'autres sources, telles que les annuaires téléphoniques et les enquêtes auprès de consommateurs, pour dresser le profil de régions particulières.

Lorsqu'elles peuvent identifier un groupe relativement homogène dans une région géographique donnée, les sociétés de marketing peuvent cibler des individus dans le groupe, les sollicitant pour divers motifs, allant des services financiers à des œuvres de bienfaisance.

Les dommages potentiels dépassent largement les simples inconvénients. Qu'on pense aux effets possibles d'une étude statistique menée dans un petit quartier qui a un taux élevé de troubles mentaux, par exemple, ou d'une étude sur un groupe identifiable dont le taux d'infection au VIH est élevé.

J'ai soulevé mes réserves à ce sujet auprès de Statistique Canada, qui m'a répondu que bien qu'il fasse tout en son pouvoir pour s'assurer que les individus ne peuvent être identifiés dans l'une ou l'autre de ses publications statistiques, il a établi un groupe de travail visant à déterminer les mesures à prendre pour aborder justement les questions touchant la protection des renseignements collectifs. Statistique Canada a signifié sa volonté de collaborer avec mon personnel pour explorer cette question plus avant. Je me réjouis de poursuivre plus amplement des discussions avec Statistique Canada sur cette question.

Un nouveau système électronique à la Défense nationale a compromis la vie privée de milliers de personnes

Le fait de ne pas avoir pris en considération l'incidence sur la vie privée d'un nouveau système électronique d'information a entraîné l'accès possible par n'importe quel employé du ministère de la Défense nationale (MDN) aux renseignements personnels de milliers de membres du personnel militaire. Cette situation aurait pu être évitée si des mesures de sécurité simples avaient été en place.

Ce cas est un exemple classique de la facilité avec laquelle la vie privée peut être compromise même avec de bonnes intentions d'accroître l'efficacité de la gestion.

Le MDN voulait donner aux gestionnaires un outil qui leur permettrait de gérer leur personnel plus efficacement. Toutefois, les agents de projet n'ont pas consulté le coordonnateur de la protection des renseignements personnels du Ministère afin d'assurer que le système était conforme aux exigences de la *Loi sur la protection des renseignements personnels*.

Par conséquent, n'importe quel employé du MDN pouvait visiter le site des ressources humaines sur le réseau informatique interne du Ministère et lire ou télécharger des renseignements personnels détaillés sur les membres des Forces canadiennes. Les renseignements comprenaient la date et le lieu de naissance, l'adresse personnelle, l'état matrimonial, les noms et dates de naissance des personnes à charge, ainsi que les résultats d'épreuves de compétence linguistique.

Suivant l'intervention du Commissariat, le MDN a accepté de prendre des mesures correctives pour mettre fin à cet accès injustifié. Il a déplacé les renseignements sur un site accessible par mot de passe seulement, et les mots de passe ont été accordés suivant le principe de l'accès sélectif.

Le MDN a également affiché un message électronique sur le site des ressources humaines demandant aux utilisateurs de supprimer tout renseignement tiré de l'ancien site. Je m'inquiétais à l'idée que ce message ne joindrait pas toutes les personnes qui avaient extrait ou téléchargé des renseignements personnels de l'ancien site. J'ai donc demandé au MDN de prendre une mesure corrective supplémentaire pour relever tous les utilisateurs. Le sous-ministre adjoint, Finances et services du Ministère, a envoyé une note de service à tous les cadres supérieurs de la Défense nationale leur demandant d'avertir les employés de supprimer les renseignements personnels tirés du site des ressources humaines initial.

Il est clair, dans cette affaire, que le MDN a contrevenu aux dispositions relatives à l'utilisation et à la communication des renseignements personnels énoncées aux articles 7 et 8 de la *Loi sur la protection des renseignements personnels* et qu'il a violé le droit fondamental

des employés touchant la protection de leurs renseignements personnels. Ainsi, j'ai conclu que cette plainte était fondée. Étant que le MDN a pris des mesures correctives satisfaisantes pour respecter les exigences de la *Loi sur la protection des renseignements personnels*, je considère la plainte comme résolue.

Santé Canada ne sait pas si elle a communiqué des renseignements personnels

Un individu s'est plaint qu'un médecin à Santé Canada a indûment envoyé une évaluation psychiatrique à son sujet à son employeur, l'Agence des douanes et du revenu du Canada (ADRC). ADRC lui a demandé de se soumettre à l'évaluation de la santé et d'aptitude au travail que Santé Canada effectue pour le compte des ministères et agences fédéraux. Pour appuyer son allégation, il a fait référence à une feuille d'accompagnement de télécopie indiquant que Santé Canada avait transmis une télécopie de 11 pages à un conseiller en ressources humaines d'ADRC en octobre 1998.

Une vérification des dossiers de Santé Canada a confirmé que le médecin de Santé Canada avait de fait transmis un document de 11 pages par télécopieur à l'employeur à ce temps-là. Toutefois, l'évaluation psychiatrique du plaignant n'a pas été trouvée dans les dossiers de l'employeur. Il a été impossible de déterminer exactement ce que Santé Canada avait transmis à l'employeur ou même si la télécopie était parvenue à destination.

Si l'enquête avait confirmé que les évaluations avaient été envoyées à l'employeur, j'aurais alors exigé d'étudier les détails de la divulgation. Mon examen aurait consisté à déterminer si la divulgation était conforme aux exigences de la *Loi sur la protection des renseignements personnels*.

À mon avis, il s'agit ici d'un sérieux problème de gestion des dossiers car une institution fédérale chargée d'assurer la protection des renseignements médicaux de nature délicate n'a pu déterminer quels documents ont été transmis par télécopieur ou même si ceux-ci ont été envoyés au bon destinataire.

Pour éviter que ce problème ne se reproduise, Santé Canada a envoyé une note à tous les directeurs dans les bureaux régionaux leur rappelant que les rapports médicaux ne doivent pas être transmis par télécopieur. Dans les cas où les documents doivent être transmis par télécopieur, Santé Canada a établi un protocole à suivre afin d'assurer la protection des renseignements personnels. Le protocole prévoit les mesures suivantes :

- Le nom et le numéro de téléphone du destinataire doivent être indiqués;
- Les documents télécopiés doivent être énumérés sur la feuille d'accompagnement;
- Il faut communiquer avec le destinataire par téléphone avant d'envoyer la télécopie pour assurer que celui-ci est sur place pour recevoir les documents; et

- Le destinataire doit confirmer par écrit la réception des documents.

Ces principes doivent être respectés par toute institution qui transmet des renseignements personnels par télécopieur non sécurisé.

Des renseignements sur des permis de petite embarcation utilisés pour évaluer les taxes de vente

Un homme sur la côte ouest a acheté un petit bateau et a obtenu un permis de petite embarcation auprès d'agents de l'Agence des douanes et du revenu du Canada. Il s'est plaint que l'Agence avait partagé les renseignements sur sa demande de permis avec le ministère des Finances de la Colombie-Britannique, qui a par la suite perçu les taxes de vente provinciales sur le prix d'achat de l'embarcation. Le plaignant a affirmé qu'il ne croyait pas que les propriétaires de nouveau bateau savaient que leurs renseignements personnels étaient communiqués de cette façon.

Bien que les agents des douanes délivrent des permis de petite embarcation, ils le font pour le compte du ministère des Pêches et Océans, qui administre le *Règlement sur les petits bâtiments*, aux termes de la *Loi sur la marine marchande du Canada*.

La compétence du ministère des Pêches et Océans relative à la communication de renseignements personnels sans consentement préalable est conférée aux termes d'une entente entre les gouvernements du Canada et de la Colombie-Britannique, qui prévoit l'accès, l'utilisation et la communication de renseignements personnels afin d'administrer ou d'appliquer les lois. Cette pratique est conforme aux dispositions de la *Loi sur la protection des renseignements personnels*. C'est pourquoi j'ai conclu qu'il s'agissait d'une communication autorisée de renseignements personnels sans consentement préalable.

J'ai toutefois émis certaines réserves au sujet de la transparence de la collecte de ces renseignements. Le ministère des Pêches et Océans a accepté volontiers de modifier le processus de demande de permis de façon à informer les personnes qui achètent des embarcations que leurs renseignements seront transmis aux provinces aux fins de l'évaluation des taxes de vente. Le Ministère a également convenu de revoir l'entente afin d'en préciser le libellé.

Absence de normes touchant la communication de renseignements personnels aux médecins

Un individu s'est plaint que son employeur, l'Agence des douanes et du revenu du Canada, ait communiqué de ses renseignements personnels en trop grand nombre à un psychiatre.

L'individu en question avait présenté une demande à la Commission de la santé et sécurité au travail du Québec concernant un congé pour des motifs de stress, qui découlait présumément du milieu de travail défavorable

créé par l'employeur. L'employeur, en retour, a contesté la demande de l'employé et demandé l'avis d'un psychiatre par le biais de Santé Canada.

L'employeur a écrit au psychiatre expliquant ses réserves au sujet de l'employé et a joint à la lettre une évaluation du rendement, que l'employé avait refusé de signer, afin d'appuyer ses prétentions. Le plaignant a soutenu que l'évaluation négative n'aurait pas dû être communiquée, et il a caractérisé cette communication comme une tentative par son employeur d'influencer l'avis du psychiatre.

Selon le Protocole d'évaluation de la santé et d'aptitude au travail de Santé Canada, l'employeur doit fournir au médecin la description du problème et les motifs de sa demande d'évaluation. Toutefois le Protocole ne comprend aucune mention concernant l'envoi de documents.

La Politique sur la santé et la sécurité au travail du Conseil du Trésor du Canada ne précise pas le genre de documents à remettre aux médecins. Pas plus qu'Info Source, répertoire des fonds de renseignements personnels au fédéral et le principal outil de référence en place pour aider le public à exercer ses droits aux termes de la *Loi sur la protection des renseignements personnels*. Info Source n'aborde pas la question du recours aux évaluations aux fins des congés de maladie ou d'avis médical. Cela signifie que les gestionnaires au fédéral n'ont pas de directives sur lesquelles s'appuyer lorsqu'ils transmettent des documents aux médecins qui effectuent l'évaluation d'employés. Il s'agit d'une situation inacceptable.

À la suite des discussions entre le Commissariat et les représentants du Conseil du Trésor et de Santé Canada, le Conseil du Trésor a convenu de réviser sa Norme relative aux examens de santé, de façon qu'elle comprenne les directives suivantes :

- L'employeur doit transmettre une lettre explicative seulement au médecin.
- L'employeur doit consulter le médecin avant de transmettre des documents à l'appui.
- L'employeur ne doit ni utiliser ni communiquer les renseignements personnels de tiers lorsqu'il précise les motifs de sa demande d'évaluation.
- Lorsque la situation le permet, l'employeur doit rencontrer l'employé pour lui expliquer les motifs de la demande d'avis médical et l'informer des renseignements qui seront fournis au médecin et les raisons connexes, de façon à assurer la transparence du processus.
- L'employeur ne doit ni utiliser ni communiquer des renseignements non appuyés de documents, tels que des renseignements sur la foi d'autrui ou des commentaires d'évaluation.

Le Conseil du Trésor a également indiqué qu'il inclura ces directives dans les bulletins qu'il prépare à l'intention des coordonnateurs de l'accès à l'information et de la protection des renseignements personnels qui travaillent dans les organismes fédéraux visés par la *Loi sur la protection des renseignements personnels*.

Les renseignements personnels d'un revendicateur du statut de réfugié communiqués à un autre revendicateur

Un avocat d'immigration s'est plaint que la Commission de l'immigration et du statut de réfugié du Canada ait communiqué des renseignements personnels d'un revendicateur du statut de réfugié à un autre revendicateur. Ce qui est intéressant dans ce cas, c'est que l'avocat représentait indépendamment les deux clients. La Commission lui a donné le Formulaire de renseignements personnels de la femme, qui l'a complété au point d'entrée pour appuyer sa revendication de statut de réfugié, à titre d'avocat-conseil de son ex-conjoint lors des processus d'audience.

Les deux individus s'étaient présentés ensemble au point d'entrée et avaient indiqué à ce moment-là qu'ils étaient conjoints de fait. La Commission a soutenu que les détails qu'ils avaient tous deux fournis dans leur revendication étaient pertinents et servaient à évaluer non seulement leur crédibilité personnelle, mais également celle de leur conjoint. La Commission a soutenu que l'utilisation des renseignements personnels dans les deux revendications était conforme aux fins initiales pour lesquelles les renseignements avaient été recueillis, c'est-à-dire évaluer leurs revendications respectives de statut de réfugié. J'ai convenu et conclu que la plainte n'était pas fondée.

Néanmoins, ce cas a soulevé d'importantes questions. L'avocat-conseil a fait état de préoccupations concernant les femmes, particulièrement celles victimes de mauvais traitements, dont la revendication du statut de réfugié se fait conjointement à celle d'autres membres de la famille. Il pourrait en découler qu'une femme communique des détails de nature délicate et intime sur les mauvais traitements infligés en salle d'audience où se trouvent de nombreux parents ou anciens parents. Cette expérience pourrait être difficile, voire traumatisante, et porter atteinte à la vie privée d'un individu.

Le processus en vigueur à la Commission prévoit de dispositions dans de telles circonstances. Les revendicateurs peuvent présenter une demande pour que les revendications soient traitées séparément. Je me réjouis d'apprendre que dans cette affaire la Commission a retiré le Formulaire de renseignements personnels rempli par la femme lorsque son avocat s'y est opposé.

Il y aura amélioration apporté au Formulaire de renseignements personnels avec l'ajout d'un paragraphe qui avertit clairement les revendicateurs du statut de réfugié de l'utilisation possible de leurs renseignements personnels lors d'une autre audience.

Jurys de sélection et notes manuscrites

La *Loi sur la protection des renseignements personnels* énonce clairement que les renseignements personnels utilisés par une institution fédérale en vue de prendre une décision administrative au sujet d'un individu doivent être mis à la disposition de cet individu et être conservés pour une période minimale de deux ans.

Cette disposition s'applique aux notes manuscrites que les membres du jury de sélection prennent durant les entrevues pour combler un poste. Les membres du jury de sélection écrivent leurs notes au moment de prendre une décision concernant l'admissibilité à un poste d'un individu en particulier. Cela signifie que les notes ont été utilisées à des fins administratives et doivent être conservées pendant au moins deux ans. Cette question a été abordée dans plusieurs rapports déposés par mon prédécesseur.

Dans cette affaire, un candidat qui n'a pas été retenu pour un poste à Pêches et Océans Canada a demandé d'avoir accès aux notes manuscrites d'origine qu'avaient prises les membres du jury de sélection afin de préparer un appel touchant le concours. Le Ministère a répondu à sa demande en lui fournissant un exemplaire du rapport sommaire dactylographié des notes des membres du jury, en précisant que les notes d'origine avaient été détruites une fois le concours terminé.

Après délibération, le Ministère a reconnu le bien-fondé de mon opinion, à savoir qu'il lui incombe de conserver dans ses dossiers l'original des notes. Des fonctionnaires du Ministère ont affirmé qu'ils n'ont pas délibérément refusé l'accès aux renseignements personnels et m'ont assuré que les politiques avaient été modifiées de façon que les notes d'origine des membres du jury de sélection sont conservées dans les dossiers de dotation.

Le courrier électronique personnel n'est pas nécessairement privé

Un employé du ministère de la Défense nationale (MDN) s'est demandé si son employeur était autorisé à utiliser et à communiquer ses messages électroniques privés dans une enquête visant une plainte de harcèlement, alors que ces messages électroniques avaient été indûment recueillis.

Une personne avait eu accès à l'ordinateur du plaignant et avait téléchargé bon nombre de ses messages électroniques. Ceux-ci renfermaient des renseignements personnels

sur le plaignant ainsi que des commentaires dérogatoires au sujet de collègues. Les messages ont été imprimés et laissés sur le bureau de plusieurs employés. Après avoir lu ces messages, les employés en cause en ont donné copie à leur supérieur et ont déposé une plainte de harcèlement contre le plaignant.

L'employeur a retenu les services d'un consultant pour enquêter sur les plaintes de harcèlement et lui a remis copie des messages électroniques qui lui servirait de preuve pour appuyer son enquête. (Une enquête distincte n'a pas permis de déterminer qui avait téléchargé les messages.)

Lorsque le plaignant a appris que ses messages électroniques avaient été remis au consultant, il s'est plaint au Commissariat en affirmant qu'ils avaient été obtenus de façon inconvenante en premier lieu et que l'employeur n'avait pas le droit de s'en servir dans l'enquête sur les plaintes de harcèlement ou de les remettre au consultant.

Cette affaire a soulevé des questions importantes et opportunes. Bien qu'il ne s'agisse pas d'une enquête criminelle, cette situation porte toutefois à réfléchir sur l'utilisation, lors d'une enquête, d'éléments de preuve qui ont été obtenus de façon injuste, douteuse et possiblement illicite.

Cela soulève la question générale de la surveillance en milieu de travail et particulièrement le respect de la confidentialité des communications électroniques, dossier chaud ces dernières années. Comme je l'ai mentionné plus tôt dans le présent rapport, les employeurs soutiennent souvent que la surveillance des communications électroniques est justifiée en raison de la nécessité de protéger les employés contre le harcèlement.

Je crois fermement que les employeurs doivent assurer une telle protection. Mais je ne crois pas que cette protection se traduise nécessairement par la surveillance générale des communications électroniques ou de l'utilisation des ordinateurs. Il faut accepter qu'il y a des limites contraignantes au droit d'un employeur de lire le courrier des employés ou d'écouter leurs conversations téléphoniques ou vider leurs tiroirs. Je crois qu'il faut regarder de près les communications électroniques afin de déterminer les principes à appliquer à leur sujet.

La *Politique d'utilisation des réseaux électroniques* du Conseil du Trésor du Canada repose sur le postulat que la *Charte des droits et libertés* assure la protection de la vie privée des employés. Elle prévoit que les institutions mettent en place leur propre politique sur l'usage des réseaux électroniques. Elle précise également que la politique doit établir les usages autorisés et acceptables des réseaux. La politique du Conseil du Trésor n'interdit pas la surveillance dans certaines conditions particulières.

La politique du MDN sur la gestion du courrier électronique précise que les employés ne peuvent s'attendre au respect de leur vie privée lorsqu'ils utilisent les systèmes de courrier électronique. Je trouve cela particulièrement déplorable. La loi en matière de la protection de la vie privée a été élaborée en se fondant sur la notion d'« attentes raisonnables de respect de la vie privée », et l'une des façons dont les tribunaux déterminent s'il y a eu violation de la vie privée est d'établir tout d'abord si une personne peut raisonnablement s'attendre à ce que sa vie privée soit respectée à un endroit et à un moment donnés. Mais je ne suis pas d'accord qu'en raison de ce principe on porte atteinte à la vie privée d'un employé ou de quiconque en lui disant simplement qu'il ne peut s'attendre au respect de celle-ci. Bien que la gestion ait le droit et la responsabilité de gérer, elle doit toutefois le faire en tenant compte de certaines contraintes, y compris le respect des droits fondamentaux. Il ne revient pas à la direction seulement de déterminer si l'attente en matière de respect de la vie privée est raisonnable.

Dans cette affaire, j'ai conclu que l'employeur n'avait pas contrevenu aux dispositions de la *Loi sur la protection des renseignements personnels*, et, ce qui est peut-être plus important, qu'il n'avait pas agi de façon déraisonnable dans les circonstances. Je crois que l'attente au respect de la vie privée du plaignant ne pouvait être satisfaite lorsque ses messages électroniques se sont retrouvés entre les mains de ses collègues. La façon dont cela s'est produit, à tort ou à raison, n'est pas en cause ici, et je n'ai trouvé aucune preuve que le gestionnaire ou supérieur du plaignant a surveillé son courrier électronique ou qu'il a indûment eu accès au courrier.

L'employeur était autorisé à embaucher un consultant pour mener l'enquête sur les plaintes de harcèlement, et j'ai conclu qu'il avait le droit de remettre les messages électroniques au consultant. Comme les plaintes reposaient sur ces messages, l'employeur n'aurait raisonnablement pu refuser de les donner au consultant.

Enfin, j'ai informé le plaignant que les employés qui se servent du réseau électronique de l'employeur de façon qui contrevient à la politique ministérielle – dans la présente affaire, écrire des messages dérogatoires au sujet de collègues, ce qui peut être perçu comme une forme de harcèlement – ne peuvent s'attendre à ce que leurs supérieurs ignorent ce comportement inconvenante lorsque celui-ci est porté à leur attention. De nouveau, la façon dont on a renseigné le supérieur à ce sujet n'est pas en cause. S'il avait été démontré que les gestionnaires ou les supérieurs avaient de fait accédé au courrier électronique du plaignant, il se peut fort bien que j'aurais perçu cette affaire différemment.

Incidents visés par la *Loi sur la protection des renseignements personnels*

Un incident est une affaire qui est portée à mon attention et qui doit faire l'objet d'une enquête, sans toutefois constituer une plainte officielle en vertu de la *Loi sur la protection des renseignements personnels*. Durant la période visée par le présent rapport, nous avons examiné 21 incidents dont j'ai eu connaissance de diverses sources. La majorité de ces incidents concernaient la communication par inadvertance de renseignements personnels ou de présumées violations à la *Loi sur la protection des renseignements personnels*. Les exemples les plus frappants sont présentés dans les lignes qui suivent.

L'ouverture du courrier – le droit à la vie privée doit être la première considération

En mars 2001, il a été révélé que des fonctionnaires de l'Agence canadienne des douanes ouvraient du courrier qui arrivait au Canada et qu'ils transmettaient les renseignements à Citoyenneté et Immigration Canada. Le caractère sacré de la correspondance personnelle est une pierre angulaire de la vie privée, et les Canadiens et Canadiennes s'attendent à ce que le courrier soit seulement ouvert par le destinataire prévu. Nous n'habitons pas un pays où les autorités ouvrent couramment le courrier, ou du moins c'est ce que nous croyions. Je me suis immédiatement penché sur cette affaire.

De nombreuses personnes étaient surprises d'apprendre que l'ouverture du courrier par un agent des douanes était licite, dans la mesure où l'envoi postal pèse plus de 30 grammes. Si le courrier pèse moins de 30 grammes, la *Loi sur les douanes* interdit de l'ouvrir, à moins d'avoir un mandat de perquisition ou le consentement du destinataire. Mais dans la mesure où le courrier pèse plus de 30 grammes, qu'il s'agit d'un colis ou de correspondance personnelle, les inspecteurs des douanes peuvent l'ouvrir s'ils croient qu'il contient des articles de contrebande ou de faux documents. Tout envoi considéré suspect du point de vue de l'immigration est remis aux agents d'immigration aux fins d'examen et de mesures ultérieures.

J'ai de sérieuses réserves au sujet de cette distinction arbitraire et artificielle en matière de poids, qui permet d'ouvrir non seulement des colis mais aussi la correspondance privée. Celle-ci doit être traitée avec le plus grand respect de façon à protéger la vie privée. Le poids de la correspondance ne devrait pas faire de différence. Pour envoyer une lettre par « messagerie prioritaire », il faut la mettre dans une grande enveloppe plutôt lourde, qui souvent fait que l'article entre dans la catégorie « de plus de 30 grammes ». Une lettre reste une lettre et la protection des renseignements qu'elle contient doit être assurée même lorsque l'expéditeur choisit un mode de livraison rapide et sûr ou que celle-ci est plus volumineuse et lourde.

J'ai indiqué mes réserves à ce sujet à la ministre de Citoyenneté et Immigration, et j'ai fait les recommandations suivantes :

- Lorsque les agents des douanes découvrent un objet solide et qui semble ne pas être de la correspondance dans une enveloppe pesant plus de 30 grammes, le fait de l'ouvrir est considéré comme une activité habituelle du processus en vigueur à l'Agence des douanes.
- Lorsque les agents ne trouvent pas d'objet solide et que l'enveloppe est retenue seulement parce qu'ils soupçonnent qu'elle peut contenir des documents frauduleux, l'Agence des douanes doit remettre le courrier sans l'ouvrir au représentant d'Immigration. Ce dernier peut alors obtenir un mandat pour l'ouvrir s'il a des motifs raisonnables de le faire.

La ministre de Citoyenneté et Immigration a rejeté ces recommandations, indiquant la difficulté apparente à constater la présence d'objets solides, comme des cartes laminées dans des enveloppes, ainsi qu'en raison du fort volume de courrier acheminé par les centres postaux. Essentiellement, elle a soutenu que la mise en œuvre des recommandations exigerait beaucoup plus de ressources.

Parce qu'il m'a été impossible d'en arriver à un consensus avec la ministre de Citoyenneté et Immigration, je me suis adressé au ministre responsable de l'Agence des douanes et du revenu du Canada. Mes entretiens avec le ministre du Revenu national ont porté fruit. L'Agence a modifié ses politiques et ne tient pas compte à présent du poids des enveloppes de type courrier à savoir si l'envoi postal pèse plus ou moins de 30 grammes. Les lettres à l'intérieur des colis sont traités comme du courrier personnel et ne sont pas ouvertes si ces lettres pèsent moins de 30 grammes. J'ai grandement apprécié l'aide du ministre du Revenu national pour résoudre cette affaire.

Santé Canada et sa liste de présumés utilisateurs de marijuana

Santé Canada a communiqué avec le Commissariat après avoir reçu l'appel d'une journaliste qui disait avoir obtenu les noms de 128 individus qui avaient présenté une demande au Ministère afin d'être exemptés en vue de se procurer de la marijuana à des fins médicales.

Mon enquête a porté sur deux questions : déterminer quelles étaient le nom des personnes sur la liste de façon à les aviser que leurs renseignements personnels avaient été compromis, et savoir comment la journaliste avait obtenu cette liste.

La journaliste a refusé de remettre la liste au Commissariat ou à Santé Canada. Comme plus de 160 personnes avaient fait une demande pour l'exemption relative à la marijuana lorsque cette affaire a été révélée, il était impossible de déterminer l'identité des 128 personnes sur la liste de la journaliste. Santé Canada n'a pas eu le choix et a dû informer tous les individus du fait qu'elle n'avait pas protégé leurs renseignements personnels.

Afin d'identifier la source de la fuite, Santé Canada a mené une enquête à l'interne. Elle a trouvé que sa sécurité était inadéquate. Presque tous les employés du Bureau de substances contrôlées avaient eu accès aux noms sur la liste. Les recommandations en vue d'améliorer la sécurité ont été mises en œuvre rapidement. Maintenant, la base de données est visée par un accès sélectif et son utilisation est restreinte par mot de passe.

En ce qui concerne la liste même, suivant l'intervention du Commissariat, la journaliste a convenu de la détruire. La liste n'a pas été publiée et la journaliste a confirmé qu'elle n'en avait pas fait de copie.

J'ai été satisfait des mesures de sécurité mises en œuvre par Santé Canada et de ses efforts pour sensibiliser les employés à leurs obligations aux termes de la *Loi sur la protection des renseignements personnels*.

Vol de demandes remplies de permis d'armes à feu à Justice Canada

Dans le cadre de ses efforts pour promouvoir l'enregistrement des armes à feu, le Centre canadien des armes à feu de Justice Canada offre un programme d'extension, afin de joindre les propriétaires d'armes à feu dans leur collectivité. Par le biais de services dans les centres commerciaux et de cliniques mobiles qui se rendent dans les petites villes et les foires rurales, le personnel aide les gens à remplir une demande de permis d'armes à feu et poste les formulaires remplis à un centre de traitement des permis. En Colombie-Britannique, une des cliniques mobiles a été volée. Celle-ci a été retrouvée, mais la boîte qui contenait quelque 20 demandes remplies manquait.

À la suite de reportages dans les médias sur cet incident, j'ai demandé qu'on fasse enquête sur les circonstances du vol ainsi que sur les efforts déployés par le Centre pour identifier et aviser les demandeurs dont les formulaires manquaient. Non seulement des renseignements personnels avaient disparu, mais des individus malhonnêtes pouvaient se servir de ces renseignements pour obtenir des permis d'armes à feu auxquels ils n'avaient pas droit.

Le Centre a lancé un appel dans les médias aux individus qui avaient rempli une demande durant les jours qui ont précédé le

vol pour qu'ils se fassent connaître. Seulement deux l'ont fait. Nous espérons que d'autres demandeurs communiqueront avec le Centre lorsqu'ils tarderont à obtenir leur permis. Par mesure de protection à long terme, le Centre a mis à jour sa politique pour assurer que les demandes remplies sont postées au Centre canadien des armes à feu en fin de journée. Bien que cet incident ne soit toujours pas réglé, je suis satisfait des efforts déployés par le Centre pour tâcher de réparer sa bévue.

Des préoccupations au sujet d'une technologie d'identification biométrique

La technologie biométrique, qui identifie les personnes suivant leurs caractéristiques physiques, est d'intérêt spécial pour le Commissariat. Lorsque les médias ont signalé que la GRC se servait d'un logiciel de reconnaissance de visage pour surveiller les voyageurs à l'Aéroport Pearson de Toronto et pour identifier des criminels, j'ai immédiatement lancé une enquête.

Il a toutefois été révélé que ce reportage était erroné. La GRC n'utilise pas des caméras de surveillance équipées d'un dispositif d'identification biométrique, bien que le logiciel soit utilisé dans les centres de détention de la GRC à l'aéroport pour analyser les photos d'individus qui ont été arrêtés. La photo d'un individu qui a été arrêté est prise par une caméra numérique puis archivée sur le disque dur d'un ordinateur autonome. Le logiciel mesure point-à-point l'ossature du visage et compare la photo numérique de l'individu arrêté aux photos qui sont déjà stockées dans le système. Comme l'ossature ne peut être modifiée au même titre que la couleur des cheveux ou des yeux, le système permet de reconnaître les individus qui ont plusieurs identités. Essentiellement, il s'agit d'une version perfectionnée des traditionnelles photos de criminels utilisées par les forces de l'ordre.

Dans les circonstances, j'étais convaincu que le logiciel d'identification biométrique n'était pas utilisé, comme l'avaient signalé les médias, et aucune question en matière de vie privée n'a été soulevée.

Une contribuable a reçu le remboursement d'une autre personne

Une bonne idée de nouvelle est tombée entre les mains d'une journaliste du *Calgary Herald* lorsqu'elle a reçu la cotisation d'impôt sur le revenu et le remboursement d'une autre personne dans la même enveloppe que les siens.

Une enquête du Commissariat a déterminé qu'une erreur mécanique au Centre de production de Winnipeg de Travaux publics et Services gouvernementaux Canada était la

cause. Le Centre de production de Winnipeg imprime et poste les cotisations fiscales ainsi que les chèques pour le compte de l'Agence des douanes et du revenu du Canada.

Le centre est pleinement automatisé pour imprimer, couper et plier les cotisations et les chèques. Les documents sont placés dans des enveloppes, qui sont scellées. Les enveloppes ensuite scellées sont lues par un détecteur optique qui les transperce au faisceau lumineux. Un avertisseur est déclenché lorsqu'une enveloppe est trop épaisse.

Cette année toutefois, en raison de changements dans la qualité du papier utilisé et le nombre d'exemplaires du formulaire, les enveloppes sont plus épaisses. Le détecteur optique n'a pu être adapté pour tenir compte de ces changements et il était inopérable.

Seulement un incident de ce genre a été signalé. Afin d'assurer que cela ne se reproduise pas, le Centre a amélioré son processus de contrôle de la qualité et a accru l'échantillonnage aléatoire des produits finals.

J'étais satisfait des mesures prises par Travaux publics pour prévenir des erreurs futures et qu'il ait présenté des excuses à l'individu concerné.

Communications dans l'intérêt public

Aux termes de l'alinéa 8(2)*m*) de la *Loi sur la protection des renseignements personnels*, le dirigeant d'un ministère peut communiquer des renseignements personnels sans le consentement de l'individu lorsque l'intérêt public contraignant l'emporte sur l'atteinte à la vie privée d'un individu ou lorsque la communication est à l'avantage de l'individu. L'« intérêt public contraignant » concerne souvent une question de sécurité et de sûreté publiques, ou l'obligation des ministères de rendre compte au public des décisions qu'ils ont prises.

Les dirigeants des ministères sont tenus, aux termes du paragraphe 8(5) de la *Loi*, de m'aviser par écrit de tout recours à cette disposition. Idéalement, ils le font avant la communication des renseignements. Le cas échéant, je peux aviser l'individu concerné de la divulgation des renseignements. Dans tous les cas, je veille à ce que seuls les renseignements personnels nécessaires soient communiqués de façon à atteindre l'objectif d'intérêt public visé.

Durant la période visée par le présent rapport annuel, on m'a avisé de 53 cas de ces communications.

L'an dernier, la majorité des avis me sont parvenus de la GRC, de la Défense nationale, du Service correctionnel Canada et de la Commission nationale des libérations conditionnelles.

La GRC a fait un nombre de communications dans l'intérêt public concernant la libération de délinquants sexuels dans la collectivité lorsque ceux-ci avaient purgé leur peine. Dans la majorité des cas, les délits sexuels avaient été commis à l'endroit d'enfants, et les délinquants présentaient des risques élevés de récidive. Certains étaient même considérés comme des délinquants sexuels dangereux. En raison des préoccupations à l'endroit des citoyens dans les collectivités où les délinquants ont été libérés, la GRC était d'avis que la communication au public des renseignements personnels sur ces délinquants compensait les préjudices causés par l'atteinte à la vie privée de ces derniers.

À plusieurs reprises, la Défense nationale a communiqué des renseignements relatifs au décès de membres en exercice des Forces canadiennes. Les renseignements ont été communiqués aux plus proches parents pour des motifs de compassion, en espérant qu'une meilleure compréhension des circonstances entourant le décès de leurs proches les aiderait à vivre leur deuil.

Service correctionnel du Canada et la Commission nationale des libérations conditionnelles ont fait paraître un nombre de rapports de la Commission d'enquête touchant des questions telles que les évasions d'établissements fédéraux, la violation des conditions de la libération d'office, et la récidive de délinquants, y compris le meurtre, une fois libérés. Ces rapports comprenaient des renseignements personnels. La majorité des cas ont beaucoup retenu l'attention des médias. Les individus ont été réincarcérés, mais en raison de la couverture médiatique et de l'attention du public, Service correctionnel du Canada et la Commission nationale des libérations conditionnelles étaient d'avis qu'il était dans l'intérêt du public de communiquer ces rapports. Ces communications étaient perçues comme nécessaires pour que le public puisse comprendre les événements entourant les incidents et les mesures prises pour empêcher qu'ils se reproduisent.

Dix premiers ministères selon le nombre de plaintes reçues
1er avril 2000 - 31 mars 2001

Organisation	Total	Accès aux renseignements personnels	Délais	Atteinte à la vie privée	Autre
Service correctionnel du Canada	672	136	342	194	
Agence des douanes et du revenu du Canada	197	91	59	47	
Développement des ressources humaines Canada	190	63	88	39	
Gendarmerie royale du Canada	136	85	24	26	1
Défense nationale	100	40	46	14	
Citoyenneté et Immigration Canada	90	32	48	10	
Centre canadien du renseignement de sécurité	40	37	2	1	
Société Postes Canada	38	16	4	18	
Justice Canada	30	8	12	10	
Affaires étrangères et Commerce international Canada	27	4	23	0	
Autres	193	97	42	54	
Total	**1 713**	**609**	**690**	**413**	**1**

Enquêtes terminées et résultats selon le ministère ou l'organisme
1er avril 2000 - 31 mars 2001

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Agriculture et Agroalimentaire Canada	0	0	0	0	0	5	5
Bureau du vérificateur général du Canada	1	0	1	0	0	0	2
Agence des douanes et du revenu du Canada	64	15	57	6	28	60	230
Société canadienne d'hypothèques et de logement	0	0	0	0	0	1	1
Société canadienne des ports	0	0	0	2	0	0	2
Société Postes Canada	5	1	5	0	2	11	24
Agence canadienne d'évaluation environnementale	0	0	0	0	0	1	1
Agence canadienne d'inspection des aliments	0	0	0	1	0	2	3
Commission canadienne des grains	0	0	0	1	0	0	1
Patrimoine canadien	0	0	1	0	0	3	4
Service canadien du renseignement de sécurité	0	2	43	0	0	2	47
Bureau du directeur général des élections	0	0	0	1	0	2	3
Citoyenneté et Immigration Canada	35	7	21	7	0	12	82
Commissariat aux langues officielles	0	0	0	1	0	0	1
Service correctionnel du Canada	262	23	59	48	2	63	457
Environnement Canada	0	0	0	0	0	4	4
Finances Canada	1	0	0	0	0	0	1
Pêches et Océans Canada	0	0	1	0	0	1	2

Enquêtes terminées et résultats selon le ministère ou l'organisme (suite)
1er avril 2000 - 31 mars 2001

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Affaires étrangères et Commerce international Canada	3	0	4	1	1	3	12
Santé Canada	5	0	26	1	1	2	35
Développement des ressources humaines Canada	79	4	21	14	2	37	157
Commission de l'immigration et du statut de réfugié du Canada	4	3	6	0	0	2	15
Affaires indiennes et du Nord canadien	4	0	2	0	0	5	11
Industrie Canada	0	0	5	1	0	3	9
Justice Canada	2	0	43	3	0	8	56
Bureau du Canada pour le millénaire	0	0	1	0	0	0	1
Archives nationales du Canada	1	0	7	6	2	12	28
Défense nationale	55	13	26	7	1	26	128
Commission nationale des libérations conditionnelles	1	0	3	0	0	7	11
Conseil national de recherches Canada	0	0	2	0	0	0	2
Ressources naturelles Canada	0	0	0	0	1	0	1
Bureau de l'ombudsman, Défense nationale et Forces canadiennes	1	0	0	0	0	3	4
Commission d'appels des pensions	0	0	0	0	0	1	1
Bureau du Conseil privé	0	0	3	1	0	1	5
Commission de la fonction publique du Canada	1	1	3	1	0	0	6
Commission des relations de travail dans la fonction publique	0	1	5	0	0	0	6

Enquêtes terminées et résultats selon le ministère ou l'organisme (suite)
1er avril 2000 - 31 mars 2001

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Travaux publics et Services gouvernementaux Canada	8	0	6	1	0	2	17
Commission des plaintes du public contre la GRC	0	1	1	0	0	0	2
Gendarmerie royale du Canada	18	9	51	12	4	25	119
Conseil de recherches en sciences humaines du Canada	0	0	0	0	0	1	1
Bureau du solliciteur général du Canada	0	2	11	1	0	0	14
Statistique Canada	1	0	1	0	0	0	2
Transports Canada	2	0	0	1	0	3	6
Conseil du Trésor du Canada	0	0	3	1	0	0	4
Administration portuaire de Vancouver	0	0	0	2	0	0	2
Anciens combattants Canada	0	0	3	1	0	13	17
Total	**553**	**82**	**421**	**121**	**44**	**321**	**1 542**

Enquêtes terminées selon les motifs et les résultats
1er avril 2000 - 31 mars 2001

	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Accès aux renseignements personnels	**11**	**73**	**241**	**54**	**36**	**215**	**630**
Accès	11	70	229	51	15	207	583
Correction-annotation	0	3	12	3	21	5	44
Langue	0	0	0	0	0	1	1
Frais inexacts	0	0	0	0	0	2	2
Atteinte à la vie privée	**45**	**9**	**124**	**58**	**8**	**95**	**339**
Collecte	3	0	28	33	2	32	98
Conservation et retrait	2	2	9	0	4	7	24
Utilisation et communication	40	7	87	25	2	56	217
Délais	**497**	**0**	**56**	**9**	**0**	**11**	**573**
Corrections-délais	15	0	1	1	0	0	17
Délais	473	0	31	8	0	10	522
Avis de prorogation	9	0	24	0	0	1	34
Total	**553**	**82**	**421**	**121**	**44**	**321**	**1 542**

Lieu d'origine des enquêtes terminées
1er avril 2000 - 31 mars 2001

Province / Territoire	Nombre
Terre-Neuve	5
Île-du-Prince-Édouard	3
Nouvelle-Écosse	103
Nouveau-Brunswick	50
Québec	306
Région de la capitale nationale – Québec	11
Région de la capitale nationale – Ontario	177
Ontario	347
Manitoba	82
Saskatchewan	63
Alberta	109
Colombie-Britannique	267
Nunavut	0
Territoires du Nord-Ouest	3
Yukon	9
Étranger	7
Total	**1 542**

Demandes de renseignements par type en vertu de la *Loi sur les renseignements personnels*
1er avril 2000 - 31 mars 2001

Sujet	Nombre
Adoption, généalogie, personnes portées disparues	31
Recensement	45
Dossiers criminels, pardons, exonération de l'impôt des É-U	190
E-311 Formulaire de déclaration du voyageur	39
Armes à feu	44
Fichier longitudinal sur la main-d'œuvre	68
Dossiers médicaux	91
Des députés	27
Absence de compétence fédérale	427
Loi sur la protection des renseignements personnels, interprétation et processus	6 460
Affaires publiques (médias et publications)	896
Réacheminées aux commissiaires provinciaux	1 068
Réacheminées à une autre agence fédérale	651
Réacheminées à d'autres	499
Registre des électeurs	21
Numéro d'assurance sociale	746
Autres	296
Total	11 599

Pratiques en matière de vie privée et examens

Introduction

Aux termes de l'article 37 de la *Loi sur la protection des renseignements personnels*, je suis autorisé à entreprendre, de façon aléatoire, des examens de la conformité relativement aux pratiques de traitement des renseignements personnels des institutions fédérales. Cela signifie que je procède à une vérification afin d'assurer que celles-ci se conforment aux principes qui régissent la collecte, l'utilisation, la communication, la protection, la conservation et le retrait des renseignements personnels, tels qu'établis aux articles 4 à 8 de la *Loi*.

Le Commissariat réalise des examens de la conformité aux termes de l'article 37 depuis 1984. J'ai élargi cette fonction l'an dernier, établissant la Direction des Examens et pratiques en matière de vie privée, qui me permet d'évaluer la mesure dans laquelle les organismes se conforment aux exigences établies dans la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques*. (La loi visant le secteur privé me confère des pouvoirs semblables en matière de vérification; mes activités de vérification dans le secteur privé sont discutées dans la deuxième partie du présent rapport.)

En tant qu'ombudsman, je préfère que les vérifications de la protection des renseignements personnels soient non conflictuelles, dans la mesure du possible. Idéalement, une vérification constitue une démarche coopérative et constructive qui permet d'aborder des questions avant qu'elles ne deviennent des plaintes. Les vérifications servent aux organisations qui veulent améliorer leurs pratiques de traitement des renseignements personnels. Bien que j'aie les mêmes pouvoirs en ce qui concerne les vérifications que ceux liés aux enquêtes, c'est-à-dire assigner des témoins à comparaître, faire prêter serment, et contraindre les organisations à produire des éléments de preuve, je n'y ai recours que lorsque je n'obtiens pas de collaboration volontaire.

Mon personnel de la Direction des Examens et pratiques en matière de vie privée, en plus de faire des vérifications et des examens, travaille auprès des organismes fédéraux qui cherchent à mieux comprendre les questions relatives à la conformité et les implications de leurs programmes et pratiques sur la vie privée. Il est essentiel que les ministères fédéraux explorent à fond sur la façon dont il faut protéger la vie privée avant de donner suite à leurs plans, même avec les meilleures intentions qui soient, de façon à réduire les coûts et à protéger les citoyens. Sur demande, mon personnel de la Direction étudie les nouvelles propositions de gestion de

F3

renseignements, comme des initiatives de couplage de données, la création de bases de données et les ententes de partage de renseignements avec d'autres organisations. Il s'agit d'une autre façon d'assurer que les droits à la vie privée des Canadiens et Canadiennes sont respectés.

Dans les pages qui suivent, sont décrits trois principaux cas touchant les pratiques de traitement des renseignements personnels d'institutions fédérales.

Des renseignements personnels n'ayant pas été déchiquetés – Golden West Document Shredding, Inc.

J'ai parlé de nombreuses fois de la nécessité d'instituer une « culture de la vie privée » au sein d'organisations, à la fois publiques et privées. Chaque fois que je lis un article dans une revue qui porte sur la vie privée, que je prends connaissance du programme d'une conférence, ou que j'examine le dernier sondage sur les préoccupations touchant la vie privée, l'accent est toujours placé sur le secteur privé. Bien que cet accent soit indiqué, il ne faut pas perdre de vue l'incroyable diversité de renseignements personnels que les gouvernements collectent, utilisent et partagent. En effet, bon nombre des plus sérieuses menaces à la vie privée continuent d'émaner de gouvernements.

À l'opposé des entreprises, les gouvernements ont le pouvoir de demander des renseignements personnels des citoyens. Ils recueillent ces renseignements en application de la *Loi*. Lorsqu'un organisme ou un programme gouvernemental a besoin de renseignements personnels pour donner suite à sa mission, ces renseignements seront recueillis. Les individus n'ont pas le choix dans cette situation.

En tant que citoyens, nous devons interagir avec le gouvernement afin de pouvoir participer aux programmes sociaux, bénéficier de l'aide sociale, et contribuer à l'intérêt public par les régimes fiscaux. Ce faisant, nous confions au gouvernement certains de nos renseignements personnels les plus délicats. Que nous présentions une demande à l'assurance-emploi, produisions nos déclarations de revenus, enregistrions nos armes à feu, ou remplissions les formulaires de recensement, nous ne sommes pas dans une position de force pour nous opposer à la collecte ou à l'utilisation de nos renseignements.

C'est pourquoi le gouvernement doit être particulièrement vigilant en maintenant la confiance que les citoyens accordent à sa capacité d'assurer la sécurité et la confidentialité des dossiers qui documentent leur vie ainsi que leur identité en tant que citoyens canadiens.

Le cas suivant représente un manquement clair à ce mandat public, et montre de façon flagrante ce qui peut arriver lorsque les coûts et la convenance l'emportent sur la vie privée.

Plus de 30 ministères et organismes fédéraux avaient entreposé des dossiers au Centre fédéral de documents de la région du Pacifique des Archives nationales du Canada. Le Centre détenait littéralement des tonnes de renseignements personnels de nature hautement délicate. Suivant la procédure normale, ces dossiers doivent être détruits après la période de conservation établie. Imaginez notre réaction lorsque un journaliste du *Vancouver Sun* nous a avisé qu'une entreprise du secteur privé, dont les services avaient été retenus pour déchiqueter et recycler les dossiers, vendait les documents au plus offrant – *intacts*, parce que du papier intégral rapporte davantage que du papier déchiqueté sur le marché du recyclage.

L'enquête a révélé qu'entre janvier et la mi-juillet 1998, les Archives nationales avaient envoyé plusieurs centaines de tonnes de documents à Golden West Document Shredding, Inc. à Burnaby (C.-B.) pour qu'ils soient détruits. Cela s'ajoutait aux documents que Golden West avait reçus directement d'autres institutions fédérales. La liste partielle suivante énumère certains des genres de dossiers dont il s'agissait, et montre la mesure dans laquelle la vie privée des Canadiens et Canadiennes peut avoir été compromise :

- de la Division de l'impôt de Revenu Canada, plus de 22 000 boîtes de documents, y compris des déclarations de revenus, des feuillets T4, des relevés de revenus de placement;
- de Développement des ressources humaines Canada, des demandes de prestations d'assurance-emploi, des dossiers de counseling en matière d'emploi de clients, des demandes de la sécurité du revenu et du supplément de revenu garanti;
- de Statistique Canada, des enregistrements d'emploi de recensement, des dossiers d'entrevues de recensement, des enquêtes sur l'emploi et d'autres natures;
- de Travaux publics et Services gouvernementaux Canada, des dossiers de rémunération d'employés, des registres de chèques, et des registres de paie;
- de Citoyenneté et Immigration Canada, des dossiers de cas d'immigration.

Si ces renseignements étaient tombés entre les mauvaises mains, les conséquences auraient été désastreuses pour des milliers de citoyens canadiens. Des renseignements personnels détaillés, comme les numéros d'assurance

sociale, les dates de naissance, les numéros de comptes bancaires et les adresses domiciliaires, représentent des biens valables. En ce qui concerne le crime en prolifération, connu comme le vol d'identité, ces renseignements servent aux criminels pour obtenir des cartes de crédit, ouvrir des comptes bancaires, réacheminer le courrier, louer des véhicules, et même obtenir un emploi. Les victimes du vol d'identité subissent de substantielles pertes de revenu, et doivent déployer beaucoup d'efforts pour rétablir leur solvabilité et leur réputation.

Mon personnel a obtenu des preuves contraignantes que les gestionnaires de Travaux publics et Services gouvernementaux Canada, de même que ceux des Archives nationales étaient au courant des sérieuses difficultés financières, techniques et en matière de sécurité de l'entreprise de déchiquetage, avant de lui accorder une autorisation de sécurité en vue de transporter et de déchiqueter des déchets de papier fédéraux protégés. En outre, l'entreprise qui s'est vu attribuer le marché de déchiquetage n'était même pas la même que celle qui avait présenté la soumission initiale. En effet, la soumission a été présentée par Golden West Document Shredding Inc., entreprise en faillite, et non Golden West Document Shredding (1995) Inc., à qui le marché a été adjugé. Cette incohérence n'a pas été relevée ou a tout simplement été ignorée.

L'agent de sécurité de Travaux publics qui a inspecté les installations de Golden West a conclu que celles-ci satisfaisaient à peine aux exigences minimales nécessaires afin d'accorder une autorisation de sécurité. Mais il a toutefois accordé cette autorisation après que le gestionnaire du Centre fédéral de documents des Archives nationales l'a assuré que les Archives nationales inspecteraient régulièrement les installations et signaleraient tout problème à Travaux publics.

Les inspections, comme il a été révélé, n'ont pas empêché l'entreprise de vendre les documents protégés non déchiquetés. En juillet 1998, lors d'une visite impromptue des installations de déchiquetage de Golden West, les employés de Travaux publics et des Archives nationales ont trouvé qu'environ 95 tonnes de documents protégés non déchiquetés avaient été vendus à une entreprise de rachat de papier et que ceux-ci avaient été mis en balles et préparés pour être expédiés outre-mer ainsi qu'aux États-Unis aux fins de recyclage.

La GRC a mené une enquête et a fait rapport à Travaux publics, mais le rapport n'a pas été rendu public et le Commissariat n'a pas été avisé de cette situation inquiétante. Des renseignements que nous avons obtenus auprès de la GRC dans le cadre de notre enquête indiquent qu'avant que les documents ne soient saisis de Golden West en juillet 1998, une entreprise de recyclage avait acheté quatre chargements de camion de renseignements gouvernementaux. Deux chargements avaient été expédiés par camion aux États-Unis et deux autres avaient été expédiés outre-mer, dont l'un en Corée du Sud et l'autre en République populaire de Chine. La GRC n'a pu établir si les documents avaient été déchiquetés.

Dans mes conclusions à la suite de l'enquête, j'ai convenu du bien-fondé des constatations de la GRC, c'est-à-dire que la responsabilité de cet incident incombe carrément aux Archives nationales et à Travaux publics. Tous deux n'ont pas pris de précautions convenables en retenant les services de Golden West, et ne se sont pas acquittés de leurs responsabilités qui consistent à protéger les renseignements personnels de nature hautement délicate de milliers de Canadiens et Canadiennes.

Le marché a été adjugé à Golden West après que les Archives nationales ont décidé de supprimer le service interne de destruction de déchets de papier protégés pour les ministères fédéraux. Cette décision a été prise afin de réduire les coûts, sans toutefois porter suffisamment attention à la protection de la vie privée. Le souci d'économie ne peut avoir préséance sur les obligations légales de protéger les renseignements personnels d'individus. Il incombait pleinement aux Archives nationales, qui agissaient pour le compte d'autres ministères et organismes, d'assurer la sécurité et la confidentialité de tous les renseignements jusqu'à ce que les documents soient déchiquetés. À la fois les Archives nationales et Travaux publics (en sa qualité d'adjudicateur) étaient tenus d'assurer que l'entrepreneur détruise les dossiers de façon indiquée.

Les Archives nationales ont un rôle essentiel à jouer pour assurer que les dossiers protégés du gouvernement sont convenablement détruits à la fin de leur cycle de vie. Elles doivent indiquer la voie à suivre concernant l'établissement de normes et de pratiques relatives à la gestion des dossiers et des renseignements du gouvernement du Canada. Le fait de demander aux ministères de prendre leurs propres arrangements pour éliminer les déchets protégés augmente considérablement les risques. Cet incident ne se serait jamais produit si les Archives nationales avaient continué de déchiqueter les déchets au centre régional de documents ou si les fonctionnaires avaient surveillé en tout temps les opérations de déchiquetage.

Dans une perspective de gestion des risques, la meilleure solution consisterait à rétablir le déchiquetage des dossiers de nature délicate dans les locaux des Archives nationales. Une solution de rechange consisterait à recourir aux services de déchiquetage privés de l'extérieur, mais seulement s'ils peuvent garantir des mesures de sécurité convenables, et seulement dans la mesure où le déchiquetage fait l'objet d'une surveillance constante par le personnel des Archives nationales. Je me rends compte des implications substantielles touchant les ressources associées à ces solutions pour les Archives nationales, et je suis prêt à discuter de toute autre proposition qui s'avérerait aussi efficace.

Suivant les conclusions dans cette enquête, j'ai formulé une série de recommandations aux Archives nationales et à Travaux publics, et je leur ai demandé de présenter un rapport au Commissariat sur les façons envisagées pour donner suite à ces recommandations. Je leur ai également demandé d'informer à l'avenir le Commissariat sans délai relativement à toute communication accidentelle ou incorrecte de renseignements personnels.

De plus, j'ai averti les deux organismes que j'informerai le Conseil du Trésor, qui est chargé d'établir la Politique sur la sécurité du gouvernement du Canada et de veiller à ce que les ministères la respectent, de mes inquiétudes au sujet de la sécurité et de la confidentialité des renseignements personnels qui doivent être éliminés. Le Conseil est donc convenu d'examiner avec soin les recommandations de mon rapport qui concernent soit la Politique sur la sécurité soit la norme particulière sur la sécurité des contrats dans le contexte de l'examen en cours de la Politique sur la sécurité du gouvernement du Canada, en vue de diminuer les risques qu'un tel incident se reproduise.

Préoccupations en matière de vie privée du Programme canadien des armes à feu

Le Commissariat s'est beaucoup intéressé au Programme canadien des armes à feu depuis la mi-1990 – bien entendu parce que le Programme vise la collecte et l'utilisation de quantités considérables de renseignements personnels de nature hautement délicate. Le Commissariat a cerné un nombre d'inquiétudes potentielles en matière de vie privée lorsque le concept avait initialement été proposé, suggérant plusieurs modifications afin de protéger la vie privée lorsque le projet de loi était à l'étude au Parlement, et donnant des commentaires ultérieurs lorsque le règlement a été annexé aux mesures législatives. Aucune de nos suggestions n'a été retenue.

Le Commissariat continue de recevoir de nombreuses demandes de renseignements et plaintes au sujet du Programme, y compris de députés. Mon prédécesseur a entrepris un examen en janvier 2000 des pratiques de traitement des renseignements personnels du Programme. Cet examen est maintenant terminé. À la lumière de ce qui a été révélé, mes principales préoccupations liées à la vie privée qui touchent le Programme se rapportent à deux domaines : les droits d'accès et de correction, et la collecte et l'utilisation des renseignements personnels.

Le droit d'accès et de correction est très important parce que des renseignements inexacts ou non corroborés dans la base de données Personnes d'intérêt – Armes à feu, par exemple, peuvent entraîner des délais, la non-délivrance de permis, et l'interrogation de voisins ou de connaissances. (La base de données Personnes d'intérêt – Armes à feu a été créée en 1998 afin de satisfaire aux objectifs de l'article 5 de la *Loi sur les armes à feu* touchant l'inadmissibilité à un permis. Plus de 900 organismes d'application de la *Loi* partout au Canada entrent des codes de déclaration d'incidents dans le Réseau du Service national de police, qui servent ensuite d'indicateurs dans la base de données dans le cadre du processus d'examen des demandes.)

Les individus qui veulent exercer leur droit d'accès et de correction de leurs renseignements personnels conservés par le Programme canadien des armes à feu trouvent qu'il est difficile de le faire et ils doivent y consacrer beaucoup de temps. La nature multijuridictionnelle du Programme fait que ces derniers doivent parfois se rendre à plusieurs ministères ou organismes ou à différents paliers de gouvernement pour accéder à leurs renseignements personnels.

Un résidant de l'Ontario, par exemple, où des lois provinciales et municipales sur la vie privée sont en vigueur, peut être tenu de présenter jusqu'à trois demandes d'accès distinctes pour obtenir les renseignements personnels se rapportant à une demande de permis d'armes à feu qui est présentée au palier fédéral. La situation est pire pour les résidants de l'Île-du-Prince-Édouard, qui n'ont toujours pas de droit d'accès autorisé en vertu d'une loi à leurs renseignements personnels détenus au niveau provincial.

Concernant la collecte et l'utilisation des renseignements personnels, mon examen a révélé que les mesures de contrôle limitant l'accès au Système de récupération de renseignements judiciaires, par exemple, sont inadéquates. Les agents aux armes à feu ont

accès à plus de renseignements que ceux dont ils ont besoin pour prendre des décisions concernant l'admissibilité des demandeurs. Ils ont également accès à des renseignements personnels sur d'autres individus, comme des témoins, des connaissances et des victimes. Ces derniers ne présentent pas de demande de permis. Ces renseignements à leur sujet ne seraient normalement pas pertinents suivant les exigences du Programme.

Un autre problème découle du fait que les préposés aux armes à feu se fient aux renseignements recueillis dans le Système de récupération de renseignements judiciaires sans en vérifier l'exactitude auprès du service de police d'origine. Cela est contraire à la fois aux politiques établies de la GRC et au paragraphe 6(2) de la *Loi sur la protection des renseignements personnels*, qui prévoit que les renseignements personnels soient exacts, à jour et complets. L'examen a également révélé que certains des renseignements recueillis dans les bases de données de la police pour le système Personnes d'intérêt – Armes à feu se rapportent à des incidents qui ne sont pas admissibles aux termes de l'article 5 de la *Loi sur les armes à feu* ou qui sont fondés sur des renseignements non corroborés.

J'ai également évalué les questions sur les antécédents personnels du formulaire de demande de permis d'armes à feu afin de déterminer si elles sont conformes aux restrictions de la *Loi sur la protection des renseignements personnels* visant la collecte de renseignements personnels.

À mon avis, le Programme canadien des armes à feu n'a pas démontré la nécessité de toutes les questions. J'ai des réserves au sujet de la nature d'intrusion large de ces trois questions :

- « 19d) : Au cours des cinq dernières années, avez-vous tenté ou menacé de vous suicider ou, après avoir consulté un médecin, avez-vous fait l'objet d'un diagnostic ou subi un traitement à la suite d'une dépression, d'abus d'alcool ou de drogues, de problèmes comportementaux ou émotifs?
- 19e) : Au cours des cinq dernières années, la police ou les services sociaux ont-ils, à votre connaissance, reçu une plainte contre vous pour usage, tentative ou menace de violence ou autre conflit à la maison ou ailleurs?
- 19f) : Au cours des deux dernières années, avez-vous vécu un divorce, une séparation, une rupture d'une relation importante, ou encore avez-vous perdu un emploi ou fait faillite? »

J'ai recommandé que que les questions des paragraphes 19 d) et 19 f) soient éliminées et que celle du paragraphe 19 e) soit modifiée pour éliminer les références telles que « autre conflit » et « ailleurs » afin d'évacuer toute ambiguité.

Bien que mon examen ait également soulevé certaines questions touchant la communication des renseignements personnels et les mesures de sécurité, il a été révélé que les mesures de sécurité matérielles, personnelles et en matière de technologie de l'information conviennent aux renseignements protégés. Toutefois, l'examen a montré que le Programme canadien des armes à feu n'a toujours pas adopté de politiques, procédures et pratiques touchant la conservation et le retrait des dossiers du Programme.

Suivant cet examen, j'ai formulé 34 recommandations pour que des mesures correctives soient prises concernant les pratiques générales de gestion des renseignements personnels du Programme. Bien que je reçoive des commentaires positifs de la Gendarmerie royale du Canada, je n'ai toujours pas reçu de réponse du ministère de la Justice.

L'examen n'a pas abordé les questions qui ont été soulevées à la suite de la recherche et du travail sur le terrain, sur lequel s'appuie l'examen, y compris les questions d'impartition et les ententes internationales de partage de renseignements. De plus, l'examen n'a pas porté sur le traitement des renseignements personnels par l'Agence des douanes et du revenu du Canada. Depuis le 1er janvier 2001, l'ADRC est chargée d'administrer la partie de la *Loi sur les armes à feu* qui porte sur les déclarations en douanes et le mouvement des armes à feu. Au moment de l'examen, cette partie de la Loi n'était toujours pas en vigueur. Nous étudions actuellement ces aspects du Programme.

Un nouveau protocole relatif aux bases de données est adopté suivant le Fichier longitudinal sur la main-d'œuvre

Développement des ressources humaines Canada (DRHC) a démantelé le Fichier longitudinal sur la main-d'œuvre en mai 2000, après que le public s'est insurgé contre celui-ci. Depuis, DRHC a mis en œuvre un protocole rigoureux touchant tous les projets de recherche futurs entrepris par l'un ou l'autre de ses bureaux.

Le protocole s'applique à toutes les activités d'analyse, de recherche et d'évaluation qui nécessitent le couplage de bases de données séparées. Il vise également le couplage de données externes, y compris les activités avec un entrepreneur de l'extérieur. Il couvre également l'utilisation d'identificateurs personnels non masqués aux fins d'enquête, que celle-ci soit menée par DRHC, un

entrepreneur ou Statistique Canada et que la source de données soit une base de données interne (c.-à-d. de DRHC) ou externe.

Nonobstant le fait que DRHC réalisera seulement des couplages pour des analyses et recherches en matière de politique, conformément à son mandat établi dans la *Loi*, la principale caractéristique du protocole est d'établir un équilibre. Le protocole s'appuie sur des principes liés à l'intérêt public, y compris la confidentialité, la transparence, l'évaluation de l'intérêt public et l'évitement de préjudices potentiels pour les individus et les groupes identifiables.

Je me réjouis de constater que DRHC a reconnu que le couplage des données entre des bases de données distinctes constitue une intrusion flagrante à la protection de la vie privée. DRHC envisagera seulement de telles entreprises lorsque les avantages sont clairement dans l'intérêt public national. Une autre exigence tient au fait que l'objectif du projet ne doit ni être au détriment des individus concernés ou de groupes identifiables ni que le projet vise à prendre des décisions administratives à leur sujet.

Le protocole prévoit également que la diffusion d'information liée au couplage des données dans les bases soit effectuée conformément aux dispositions sur la confidentialité de la *Loi sur le ministère Développement des ressources humaines Canada*, la *Loi sur la protection des renseignements personnels*, la *Loi sur l'assurance-emploi*, la *Loi de l'impôt sur le revenu*, le *Régime de pensions du Canada*, et la *Loi sur la sécurité de la vieillesse* ainsi qu'aux critères relatifs à la communication des renseignements compris dans les ententes avec les provinces, les territoires et les autres ministères et organismes fédéraux.

Je suis également très heureux de voir que tous les liens entre les bases de données devront satisfaire à un examen et à un processus d'approbation prescrit, entre autres mesures de protection. Cela comprend la présentation de propositions documentées à un comité de spécialistes à l'interne, le Comité d'examen des banques de données, auquel siègent surtout des hauts fonctionnaires de DRHC. Le processus d'examen prévoit la consultation du Commissariat concernant tous les projets, ainsi que des partenaires à l'extérieur lorsque le projet comporte le couplage des bases de données de DRHC avec des données de l'extérieur. Enfin, la recommandation du Comité d'examen des banques de données a été transmise au sous-ministre de Développement des ressources humaines, qui est chargé d'approuver tous les projets.

DRHC travaille actuellement à l'élaboration d'un cadre de protection juridique qui régira les activités futures de collecte et d'utilisation de données et de renseignements obtenus auprès de Canadiens et Canadiennes, dont se servira DRHC pour ses besoins particuliers en matière de recherche. Le cadre comprendra des sanctions pour les mésusages et sera conforme aux lois, politiques et procédures du fédéral ainsi qu'aux constatations qui découleront de tout examen par le gouvernement de la *Loi sur la protection des renseignements personnels.*

Depuis septembre 2000, nous avons donné des commentaires à DRHC sur plus d'une douzaine de présentations, y compris l'Enquête canadienne par panel sur l'interruption d'emploi, le Programme canadien de prêts aux étudiants – Principales mesures du rendement, et le Programme de prestations d'emploi et de mesures de soutien.

Dans l'ensemble, je suis satisfait que DRHC a abordé les préoccupations que le Commissariat a soulevées concernant le Fichier longitudinal sur la main-d'œuvre dans son protocole de couplage des bases de données et son cadre de protection juridique proposé.

Examens

La Commission de l'immigration et du statut de réfugié et la Commission canadienne de sûreté nucléaire

Les examens des pratiques de traitement des renseignements personnels aux termes de l'article 37 de la *Loi sur la protection des renseignements personnels* ont été entrepris vers la fin du présent exercice à la Commission de l'immigration et du statut de réfugié et à la Commission canadienne de sûreté nucléaire. Ces examens ont compris des visites sur place dans la région de la capitale nationale ainsi que des bureaux régionaux choisis partout au Canada. Les examens seront terminés durant l'exercice 2001-2002.

Devant les tribunaux

Introduction

La Division juridique, dirigée par l'avocat général, me donne des conseils juridiques et stratégiques spécialisés ainsi qu'un soutien au contentieux touchant la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques.*

Aux termes de l'article 41 de la *Loi sur la protection des renseignements personnels,* un individu est autorisé, à la suite de mon enquête, à recourir à la Cour fédérale pour

demander la révision de la décision d'une institution fédérale qui lui a refusé l'accès à des renseignements personnels. Depuis l'entrée en vigueur de la *Loi sur la protection des renseignements personnels* en 1983 jusqu'au 31 mars 2001, 106 demandes de révision avaient été déposées à la Cour fédérale. Six d'entre elles ont été déposées l'exercice dernier.

Je suis autorisé, aux termes de l'article 42 de la *Loi sur la protection des renseignements personnels*, après avoir terminé une enquête, de présenter à la Cour fédérale un recours en révision d'une décision prise par une institution fédérale qui refusé l'accès à des renseignements personnels, dans la mesure où j'ai obtenu le consentement de l'individu qui a initialement demandé l'accès aux renseignements. Trois demandes ont été déposées par les anciens commissaires à la protection de la vie privée de 1984 à la fin de l'exercice 2001.

Les commissaires précédents et moi sommes également intervenus devant les tribunaux six fois au total depuis 1984 jusqu'à présent dans des demandes présentées par d'autres personnes aux termes de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*.

Décisions récentes

Le Commissaire à la protection de la vie privée c. le Conseil canadien des relations de travail

Il s'agit d'un appel interjeté par mon prédécesseur concernant la décision de la Section de première instance de la Cour fédérale. L'affaire portait sur les notes prises par des membres du Conseil canadien des relations de travail lors d'une audience sur une plainte relative au manquement au devoir de juste représentation. Mon prédécesseur a soutenu que les notes, qui contenaient des renseignements personnels du demandeur, relevaient de l'autorité du Conseil et étaient ainsi visées par le droit d'accès prévu dans la *Loi sur la protection des renseignements personnels*.

L'appel a été entendu le 9 mai 2000, et la décision a été rendue à l'audience.

La Cour d'appel fédérale a soutenu que les notes des membres du Conseil n'étaient pas visées par l'autorité du Conseil, tel que prévu à l'alinéa 12(1)b) de la *Loi sur la protection des renseignements personnels*. La Cour a déclaré : « Ces notes sont prises dans le cadre d'une instance quasi judiciaire non pas par des employés du Conseil, mais par des représentants du gouverneur en conseil investis de fonctions juridictionnelles qu'ils doivent exercer, non pas en qualité de mandataires du

Conseil, mais de façon indépendante par rapport aux autres membres de celui-ci, y compris le président dudit Conseil ou d'une institution fédérale. L'absence de contrôle que le Conseil peut exercer sur les notes en qualité d'institution fédérale s'explique principalement par l'application aux tribunaux administratifs du principe de l'indépendance judiciaire et de son corollaire, le principe du privilège décisionnel. »

Mon prédécesseur n'en a pas appelé de cette décision.

Le Commissaire à l'information du Canada (appelant) c. le Commissaire de la GRC (intimé) et le Commissaire à la protection de la vie privée (intervenant)

L'affaire portait sur l'équilibre entre la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*. Une liste des affectations de quatre agents de la GRC avait fait l'objet d'une demande aux termes de la *Loi sur l'accès à l'information*. Le Commissaire de la GRC a refusé de communiquer ces renseignements parce qu'ils se rapportaient aux antécédents professionnels de ces individus et qu'il s'agissait ainsi de renseignements personnels aux termes de l'alinéa 3b) de la *Loi sur la protection des renseignements personnels*. Le Commissaire à l'information a déposé un recours en révision de ce refus devant la Cour.

La question en litige consistait à déterminer si les renseignements pouvaient être communiqués conformément à la définition de « renseignements personnels » à l'alinéa 3j) de la *Loi sur la protection des renseignements personnels*, qui précise que les renseignements touchant les postes ou fonctions d'agents ou d'employés du gouvernement ne constituent pas des renseignements personnels.

La Cour d'appel fédérale a soutenu que les renseignements en litige étaient de fait des renseignements personnels sur chaque agent et qu'ils ne relevaient pas de l'exception prévue à l'alinéa j) de la définition de « renseignements personnels ».

La Cour a rejeté l'argument de la GRC, selon lequel l'exception prévue à l'alinéa j) s'applique seulement au poste qu'occupe actuellement un fonctionnaire (ou au dernier poste occupé dans le cas d'un ancien fonctionnaire). La Cour a convenu du bien-fondé de l'argument du Commissaire à l'information et de moi-même, c.-à-d. que l'alinéa j) peut s'appliquer aux postes antérieurs.

La Cour a rejeté l'argument du Commissaire à l'information, selon lequel il faut adopter une interprétation large de l'exception énoncée à l'alinéa j) pour justifier la communication des renseignements demandés. La Cour a con-

venu du bien-fondé de ma position, indiquant que l'exception devrait être interprétée d'une manière qui ne permet pas la communication des « antécédents professionnels » d'un individu.

Le Commissaire à l'information a été autorisé à interjeter appel de cette décision à la Cour suprême du Canada. Je vais demander l'autorisation d'intervenir dans cet appel.

Affaires en instance

Formulaires de déclaration du voyageur (E-311)

Les deux cas suivants portent sur la communication de renseignements personnels par l'Agence des douanes et du revenu du Canada à la Commission de l'assurance-emploi du Canada aux fins d'un programme d'appariement des données d'enquête. Les renseignements personnels en question ont été tirés de formulaires de déclaration du voyageur (E-311) présentés aux douanes par des résidantscanadiens de 1994 à 1996. L'objet de l'appariement des données était d'identifier les prestataires d'assurance-emploi qui touchent des prestations alors qu'ils sont à l'extérieur du Canada. Aux termes de la *Loi sur l'assurance-emploi*, les prestataires doivent être prêts à travailler et ils sont inadmissibles aux prestations s'ils s'absentent du Canada.

Le Commissaire à la protection de la vie privée c. le Procureur général du Canada

Il s'agit d'un appel interjeté à la Cour suprême du Canada touchant une décision de la Cour d'appel fédérale. Les questions en litige consistaient à savoir si la Cour d'appel fédérale a erré en concluant que la communication de « renseignements personnels » par l'Agence des douanes à la Commission de l'assurance-emploi du Canada était autorisée aux termes de l'article 8 de la *Loi sur la protection des renseignements personnels* et de l'article 108 de la *Loi sur les douanes*, à savoir si l'alinéa 108(1)b) de la *Loi sur les douanes* autorise le Ministre à communiquer des renseignements personnels à la Commission en vue de leur utilisation dans un programme d'appariement de données d'enquête, et si le ministre a autorisé comme il se doit la communication des renseignements personnels sur les formulaires de déclaration du voyageur à la Commission en vue de leur utilisation dans un programme d'appariement des données d'enquête.

Il s'agit d'un renvoi présentée à la Cour fédérale conjointement par mon prédécesseur et le procureur général du Canada. La Section de première instance de la Cour fédérale a donné raison à mon prédécesseur, mais non la Cour d'appel fédérale.

La Cour d'appel fédérale a rendu sa décision le 9 février 2000 à l'audience. Les principales conclusions sont les suivantes :

- L'appariement des données est autorisé par le protocole d'entente auxiliaire pour la collecte et la communication des renseignements recueillis par l'Agence des douanes sur les voyageurs, entente qu'ont conclue le 26 avril 1997 l'Agence des douanes et la Commission canadienne de l'assurance-emploi du Canada. L'alinéa 108(1)b) de la *Loi sur les douanes* confère au ministre du Revenu le pouvoir discrétionnaire d'autoriser l'entente exposée dans le protocole auxiliaire de 1997. La Cour a statué que l'autorisation antérieure accordée en 1991 par le ministre du Revenu aux termes de l'alinéa 108(1)b) de la *Loi sur les douanes* n'était pas pertinente à l'affaire dont elle était saisie.
- L'alinéa 8(2)b) de la *Loi sur la protection des renseignements personnels* doit être interprété largement. La Cour a déclaré : « Dans ce contexte, on ne peut faire autrement qu'interpréter l'alinéa 8(2)b) comme une disposition permettant au législateur de conférer à tout ministre (par exemple), au moyen d'une loi donnée, un large pouvoir discrétionnaire quant à la forme et au fond relativement à la communication de renseignements que son ministère a recueillis, ce pouvoir discrétionnaire devant naturellement être exercé conformément à l'objet de la *Loi sur la protection des renseignements personnels.* »
- Ces objectifs ont été atteints parce que le Ministre : « a estimé que la communication demandée par la Commission l'était pour un usage permis et qu'aucun renseignement autre que ceux dont la Commission avait besoin ne serait communiqué ». En outre, le protocole auxiliaire de 1997 comprend des restrictions applicables à l'utilisation des renseignements et à leur communication à des tiers ainsi que d'autres mesures comme l'établissement d'une piste de vérification et la destruction des renseignements.

Contestation en vertu de la Charte

Il s'agit d'un appel interjeté à la Cour suprême du Canada touchant la décision de la Cour d'appel fédérale. Les questions en litige sont :

- À savoir si la communication par l'Agence des douanes à la Commission de l'assurance-emploi du Canada de renseignements personnels tirés des formulaires de déclaration du voyageur et l'utilisation subséquente de ces

renseignements dans un programme d'appariement des données comme élément de preuve contre l'individu contreviennent au droit de l'individu de ne pas faire l'objet de fouille ou de saisie déraisonnable aux termes de l'article 8 de la *Charte;*

- Et si tel est le cas, à savoir si l'élément de preuve aurait dû être exempté aux termes du paragraphe 24 2) de la *Charte*, et
- À savoir si la disposition de la *Loi sur l'assurance-emploi* qui rend inadmissible aux prestations tout individu qui s'absente du Canada porte atteinte à la liberté de circulation garantie au paragraphe 6(1) de la *Charte.*

La Cour d'appel fédérale a rejeté la demande de contrôle judiciaire de la décision prononcée par le juge-arbitre nommé conformément à la *Loi sur l'assurance-emploi.* La Cour d'appel fédérale, dans une décision prononcée le 9 février 2000, a conclu que les Canadiens et Canadiennes ne peuvent raisonnablement s'attendre au respect de la vie privé touchant les renseignements inscrits sur les formulaires E-311 de manière à susciter l'application de l'article 8 de la *Charte* (droit de ne pas faire l'objet de fouille, de perquisition ou de saisie déraisonnable). La Cour a aussi statué que l'alinéa 32b) de la *Loi sur l'assurance-chômage* (l'alinéa 32b) de la *Loi sur l'assurance-emploi :* inadmissibilité aux prestations d'assurance-emploi durant une absence du Canada) ne porte pas atteinte à la liberté de circulation garantie aux termes du paragraphe 6(1) de la *Charte.*

État de la situation

Les demandes d'appel à la Cour suprême du Canada des deux décisions ont été accordées le 17 août 2000. Les deux avis d'appel ont été déposés et signifiés le 22 août 2000.

La requête pour énoncer une question constitutionnelle dans le cadre de la contestation en vertu de la *Charte* a été signifiée aux procureurs généraux de chaque province et territoire, comme le prévoit les règles de la Cour suprême du Canada. Les procureurs généraux de l'Ontario, du Manitoba et du Québec sont intervenus.

Les affaires ont été entendues le 7 novembre 2001.

Clayton Charles Ruby c. le Solliciteur général

Il s'agit d'un appel interjeté à la Cour suprême du Canada touchant une décision de la Cour d'appel fédérale. Le réquérant s'est vu refuser l'accès à des renseignements personnels le concernant dans des fichiers par le Service canadien du renseignement de sécurité. Le Solliciteur général a refusé de communiquer les renseignements demandés par le réquérant. La Section de première instance de la Cour fédérale a rejeté la demande de révision des décisions de refus. La décision a été portée en appel à la Cour d'appel fédérale où l'appel a été accueilli en partie, et les deux questions ont été renvoyées à la Section de première instance de la Cour d'appel fédérale pour une nouvelle décision.

La Section de première instance de la Cour fédérale, de même que la Cour d'appel fédérale ont examiné la constitutionnalité de l'article 51 de la *Loi sur la protection des renseignements personnels*, qui prévoit le dépôt des renseignements devant la Cour en l'absence de l'autre partie et la tenue d'une audience à huis clos. Les deux instances inférieures ont conclu que l'article 51 de la *Loi sur la protection des renseignements personnels* viole l'alinéa 2b) de la *Charte*, mais que cette violation se justifie au regard de l'article 1 de la *Charte*.

Questions soulevées dans l'appel

- À savoir si l'article 51 de la *Loi sur la protection des renseignements personnels* contrevient à l'article 7 de la *Charte* et, si tel est le cas, cette contravention est justifiée aux termes de l'article 1; et
- À savoir si la violation de l'alinéa 2b) de la *Charte* par l'article 51 de la *Loi sur la protection des renseignements personnels* est justifiée aux termes de l'article 1.

Questions soulevées dans l'appel incident

- À savoir si la Cour d'appel fédérale a interprété l'alinéa 22(1)b) de la *Loi sur la protection des renseignements personnels* si étroitement que les institutions fédérales seront incapables de protéger convenablement le nom de leurs sources de renseignements, y compris les informateurs de police; et
- À savoir si la Cour d'appel fédérale a négligé de prendre suffisamment compte des implications de l'« effet mosaïque » et de la nécessité d'interpréter les exceptions de la *Loi sur la protection des renseignements* personnels de manière à préserver la capacité du gouvernement de protéger ses sources, ses méthodes et ses techniques d'enquête ainsi que sa capacité de faire exécuter les lois du Canada.

Dans sa décision du 8 juin 2000, la Cour d'appel fédérale a soutenu que l'article 7 de la *Charte* n'était pas en cause car les mesures de protection procédurales prévues à l'article 51 de la *Loi sur la protection des renseignements personnels* ne portaient pas atteinte aux intérêts de liberté des individus. Concernant l'alinéa 2b) de la *Charte*, la Cour d'appel fédérale a soutenu que l'article 51 de la *Loi sur la protection des renseignements personnels* violait le droit de liberté de presse, mais pouvait tout de même être légitimé en tant que limite raisonnable et justifiable aux termes de l'article 1 de la *Charte*.

Une autre question prise en considération par la Cour était l'interprétation convenable de l'alinéa 22(1)b) de la *Loi sur la protection des renseignements personnels* qui autorise une institution fédérale à refuser l'accès aux renseignements personnels lorsqu'il est raisonnable de s'attendre à ce que leur communication nuise à l'application d'une loi du Canada ou d'une province ou à la tenue d'enquêtes licites. La Cour d'appel fédérale a rejeté l'argument du solliciteur général et a soutenu que l'alinéa 22(1)b) n'autorise pas le refus de communication du simple fait que celle-ci puisse comporter un effet dissuasif sur le processus d'enquête en général. La notion de préjudice énoncée à l'alinéa 22(1)b) ne dépasse pas le champ d'une enquête donnée, qu'elle soit en cours ou envisagée.

État de la situation

M. Ruby a demandé l'autorisation d'en appeler à la Cour suprême du Canada au sujet de la décision de la Cour d'appel fédérale concernant la constitutionnalité de l'article 51 de la *Loi sur la protection des renseignements personnels*. Le solliciteur général a demandé l'autorisation de présenter un appel incident de la décision de la Cour d'appel fédérale concernant l'interprétation de l'alinéa 22(1)b) de la *Loi sur la protection des renseignements personnels*. La Cour suprême du Canada a accordé les autorisations d'appel et d'appel incident le 18 janvier 2001. J'ai demandé l'autorisation d'intervenir dans cette affaire relativement à l'alinéa 22(1)b). J'ai été autorisé à le faire le 25 mai 2001. Je déposerai mes arguments, qui diffèrent de ceux des deux parties, auprès de la Cour suprême du Canada.

Le Commissariat aux langues officielles (appelant) c. Robert Lavigne (intimé)

Cette affaire est actuellement en appel devant la Cour suprême du Canada. M. Lavigne s'est vu refuser l'accès à des renseignements personnels le concernant, qui se trouvaient dans les déclarations faites par les témoins lors d'une enquête menée par le Commissariat aux langues officielles. Le Commissariat a refusé l'accès en invoquant l'exemption prévue à l'alinéa 22(1)b) de la *Loi sur la protection des renseignements personnels*.

M. Lavigne a présenté un recours en révision à la Section de première instance de la Cour fédérale concernant le refus du Commissariat aux termes de l'article 41 de la *Loi sur la protection des renseignements personnels*. Le Commissaire à la protection de la vie privée précédent et moi-même sommes intervenus à l'appui de M. Lavigne tout au long de cette affaire. Nos interventions ont porté fruit à la fois devant la Section de première instance de la Cour fédérale et la Cour d'appel fédérale.

Suivant une décision rendue à l'audience le 6 septembre 2000, la Cour d'appel fédérale a ordonné au Commissariat aux langues officielles de remettre à M. Lavigne ses renseignements personnels. La Cour d'appel fédérale s'est appuyée sur deux de ses décisions antérieures, *Rubin c. Canada (Ministre des Transports)* et *Ruby c. Canada (Solliciteur général)*, confirmant que l'exception prévue à l'alinéa 22(1)b) ne peut être invoquée que lorsqu'il y a preuve de préjudice dans le cadre d'une enquête donnée, l'exception ne peut être invoquée une fois que l'enquête est terminée, et il est interdit de refuser la communication des renseignements demandés sur la base que cette communication pourrait comporter un effet « dissuasif » sur des enquêtes futures possibles. La Cour d'appel fédérale a rejeté l'argument du Commissariat aux langues officielles, à savoir qu'une interprétation différente était justifiée dans la présente affaire en raison du mandat conféré par la *Loi* au Commissaire aux langues officielles.

Les questions en litige qui étaient soulevées à la Cour suprême sont de savoir si la Cour d'appel a erré en concluant que les dispositions relatives à l'accès prévues à la *Loi sur la protection des renseignements personnels* l'emportent sur les dispositions relatives à la confidentialité de la *Loi sur les langues officielles* et de savoir si la décision de la Cour d'appel compromet gravement la capacité du Commissaire aux langues officielles d'appliquer la *Loi sur les langues officielles*.

État de la situation

Le Commissariat aux langues officielles a déposé une demande d'autorisation d'en appeler de la décision à la Cour suprême du Canada. L'autorisation d'appel a été accordée le 19 avril 2001. Le 21 août 2001, la Cour suprême du Canada m'a autorisé à intervenir au soutien de M. Lavigne. Mes soumissions en tant qu'intervenant seront déposés au début de décembre.

Deuxième partie
Rapport concernant la *Loi sur la protection des renseignements personnels et les documents électroniques*

Introduction

L'adoption de la *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*), représente une importante étape pour le Canada. Il s'agit d'un engagement clair du gouvernment afin de protéger notre droit fondamental à la vie privée, dans une ère où celle-ci est menacée comme elle ne l'a jamais été auparavant. Les percées technologiques qui révolutionnent notre mode de faire des affaires, conjugé à la détermination des entreprises de s'accaparer des renseignements personnels, les pays dans le monde entier reconnaissent l'importance de protéger la vie privée. En raison de la *LPRPDÉ*, Canada passe au rang des chefs de file mondiaux.

La partie 1 de la *Loi* énonce les conditions dans lesquelles les organismes peuvent recueillir, utiliser ou communiquer des renseignements personnels et accorde aux individus le droit d'accès aux renseignements personnels les concernant que détiennent les organismes ainsi que le droit de correction connexe. La *Loi* établit également le processus que peuvent emprunter les individus pour déposer une plainte officielle lorsqu'ils croient que leurs droits ont été violés ou lorsque les organisations n'ont pas respecté la *Loi*, ainsi que les recours judiciaires mis à leur disposition.

Cette partie de la *Loi* est mise en œuvre en trois étapes successives. Dans la première étape, qui a débuté le 1er janvier 2001, la *Loi* vise les renseignements personnels, ceux sur la santé exceptés, qui sont recueillis, utilisés ou communiqués dans le cadre des activités commerciales ainsi que sur les employés d'entreprises fédérales. Celles-ci comprennent les banques, le secteur de la radiodiffusion, les

entreprises de transport interprovincial et les sociétés de téléphone.

La *Loi* porte également sur la communication des renseignements personnels qui sont échangés ou vendus à l'extérieur d'une province ou du pays. En outre, elle s'applique à tout le secteur commercial du Yukon, dans les Territoires du Nord-Ouest et le Nunavut, parce que toutes les entreprises locales y sont considérées comme des entreprises fédérales et sont ainsi du ressort du Parlement fédéral.

À compter du 1er janvier 2002, la *Loi* s'appliquera également aux renseignements personnels sur la santé pour ce qui est des organismes et des activités visés lors de la première étape.

À compter du 1er janvier 2004, toutes les dispositions de la partie 1 de la *Loi* auront force exécutoire partout au Canada dans le secteur privé réglementé au niveau provincial ou territorial, sauf lorqu'une province ou un territoire a promulgué une loi que le gouverneur en conseil considère comme essentiellement similaire à la *Loi sur la protection des renseignements personnels et les documents électroniques*. En l'occurrence, la loi provinciale ou territoriale aura préséance pour toute collecte, utilisation ou communication de renseignements personnels par les enterprises qui sont visées par la loi provinciale ou territoriale. Cela signifie qu'à compter du 1er janvier 2004, les droits à la vie privée des Canadiens seront protégés dans tout le secteur privé, soit aux termes de la *Loi* fédérale ou d'une loi provinciale ou territoriale essentiellement similaire.

En tant que Commissaire à la vie privée du Canada, je suis chargé du contrôle d'application des règles régissant la collecte, l'utilisation et la communication des renseignements personnels établies dans la partie 1 de la *Loi*. Je reçois des plaintes et je mène des enquêtes et, comme il est prévu dans la *Loi sur la protection des renseignements personnels*, je joue le rôle d'ombudsman, tâchant de régler les différends par la négociation. Je peux également, suivant des motifs raisonnables, vérifier les pratiques de gestion des renseignements personnels d'une organisation.

Les pouvoirs en matière d'enquête qui sont conférés au Commissariat aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques* correspondent à ceux prévus dans la *Loi sur la protection des renseignements personnels*, bien que je sois investi d'un mandat fort élargi en vue d'entreprendre des recherches sur les questions liées à la vie privée et de favoriser la sensibilisation des Canadiens à ces questions ainsi que leur compréhension.

Le présent rapport provisoire porte sur les activités associées à la *Loi sur la protection des renseignements personnels et les documents électroniques* pour la période du 1er janvier 2001 au 30 novembre 2001.

Mise à jour des lois provinciales et territoriales

Détermination d'« essentiellement similaire »

J'interpréterai une loi provinciale ou territoriale comme « essentiellement similaire » lorsqu'elle offre un degré et une qualité de protection de la vie privée égaux ou supérieurs à ceux de la *Loi* fédérale. La *Loi* fédérale constitue le seuil ou le niveau minimal. Une loi provinciale ou territoriale sur la protection des renseignements personnels doit assurer une protection au moins équivalente à celle de la loi fédérale, ou elle ne sera pas considérée comme essentiellement similaire.

Pour être considérée essentiellement similaire, une loi provinciale devra comprendre au bas mot les dix principes établis à l'Annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques.* Bien que les dix principes du code soient considérés comme intereliés et d'importance égale, j'aimerais m'attarder aux cinq éléments de la loi car ils constituent des composantes clés de la détermination de la nature essentiellement similaire d'une loi : le consentement, le critère de la personne raisonnable, les droits d'accès et de correction, la surveillance, et les voies de recours.

Consentement

Dans la mesure où la vie privée constitue le droit d'exercer un contrôle sur l'accès à sa personne et à ses renseignements personnels, il ne peut y avoir de contrôle sans consentement ni de vie privée sans contrôle.

L'exigence relative au consentement doit être le fondement de toute loi efficace sur la protection des renseignements personnels. La *Loi* fédérale précise que le consentement doit être éclairé, et que la collecte, l'utilisation et la communication des renseignements personnels sans le consentement de l'individu ne doivent se produire que dans des circonstances exceptionnelles déterminées.

Une organisation peut seulement recueillir, utiliser ou communiquer des renseignements personnels sur un individu dans la mesure où ce dernier a accordé son consentement (sauf dans des circonstances limitées établies dans la *Loi*).

Une fois recueillis, les renseignements personnels ne peuvent être utilisés ou communiqués qu'aux fins auxquelles le consentement a été accordé (sauf dans des circonstances limitées établies dans la *Loi*).

Critère de la personne raisonnable

Le critère de la personne raisonnable impose une autre contrainte importante aux organisations. La *Loi* prévoit que la collecte, l'utilisation et la communication de renseignements personnels doivent se faire seulement aux fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Entre autres, ce critère empêche les organisations d'énoncer en des termes trop larges ou vagues les fins auxquelles renseignements sont recueillis.

Droits d'accès et de correction

Les individus doivent avoir le droit d'accéder aux renseignements personnels que les organisations détiennent à leur sujet et corriger toute inexactitude (ou signaler tout désaccord au tiers qui a reçu les renseignements).

Surveillance

Lorsqu'un individu est d'avis que ses droits à la vie privée ont été violés ou que la *Loi sur la protection des renseignements personnels* n'a pas été respectée, l'individu doit pouvoir déposer une plainte à un organisme de surveillance pleinement autonome, qui est investi du mandat précis de régler les plaintes, de mener des enquêtes exhaustives, de soumettre à la médiation et à la conciliation, de formuler des recommandations ou de prendre des ordonnances. L'organisme de surveillance doit également être investi de pouvoirs d'enquête complets afin de saisir des documents, de pénétrer dans des locaux, de contraindre à témoigner et de prendre l'initiative de vérifications des pratiques d'une organisation.

Voies de recours

À la suite de mon rapport sur une plainte auprès d'une organisation, la *Loi* fédérale permet au plaignant (ou à moi-même directement) de demander une audience à la Cour fédérale du Canada. Le plaignant ou moi-même pouvons demander à la Cour d'ordonner à l'organisation en question de rectifier ses pratiques de traitement des renseignements et de rendre publiques les mesures qu'elle a prises pour le faire. Il est possible de demander à la Cour d'accorder des dommages-intérêts au plaignant.

Il est possible d'en appeler des décisions de la Cour fédérale à la Cour d'appel fédérale ainsi qu'à la Cour suprême du Canada sur autorisation.

Je suis d'avis que toute loi provinciale qui est censée être « essentiellement similaire » doit comprendre des dispositions équivalentes en matière de recours.

Initiatives législatives en vue de réglementer le secteur privé

Jusqu'à présent, le Québec est la seule province au Canada qui a adopté des mesures de protection des renseignements personnels qui touchent les entreprises qui font affaire dans la province, tel qu'il est établi dans le Code civil. Ailleurs au Canada, deux gouvernements provinciaux – celui de la

Colombie-Britannique et de l'Ontario – ont commencé à explorer des options législatives afin de réglementer la collecte, l'utilisation et la communication des renseignements personnels dans le secteur privé. En effet, d'ici le 1er janvier 2004, les gouvernements provinciaux devront avoir adopté une loi que le gouverneur en conseil estime, par décret d'exemption, essentiellement semblable à la *Loi sur la protection des renseignements personnels et les documents électroniques.*

Secteur de la santé

Les provinces de l'Alberta, du Manitoba et de la Saskatchewan ont adopté une loi sur la protection des renseignements personnels visant spécifiquement la santé. La *Loi* est actuellement en vigueur au Manitoba et en Alberta. En décembre 2000, l'Ontario a déposé son controversé projet de loi 159, *Loi sur la protection des renseignements personnels sur la santé,* qui est resté en plan au Feuilleton.

Loi pour le secteur public

La *Loi sur la protection des renseignements personnels* du Nouveau-Brunswick est entrée en vigueur en avril 2001. La *Loi sur l'accès à l'information et la protection de la vie privée* de l'Île-du-Prince-Édouard a reçu la sanction royale le 15 mai 2001, et entrera en vigueur en novembre 2002. Suivant la présentation et l'adoption de ces deux lois, toutes les provinces et tous les territoires au Canada, à l'exception de Terre-Neuve, offrent maintenant la protection réglementaire des renseignements personnels que détiennent les ministères et les organismes fédéraux.

Enquêtes

Au 30 novembre 2001, le Commissariat avait reçu 95 plaintes officielles aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques.* Au cours de la première année depuis l'entrée en vigueur de la *Loi,* les plaintes ont essentiellement visé le secteur réglementé par le fédéral, dont près de la moitié se rapportaient aux banques.

Nombre de plaintes selon le secteur
1er janvier 2001 - le 30 novembre 2001

Malgré la mise en œuvre progressive de la *Loi,* les organismes ont dû se préparer à son entrée en vigueur, et certains n'ont toujours pas intégré ses principes dans leurs pratiques d'affaires. De nombreuses plaintes ont soulevé des questions systémiques portant sur la violation des droits à la vie privée dans le secteur privé réglementé par le fédéral. Lorsqu'il était démontré que celles-ci étaient fondées, j'ai recommandé aux organisations qu'elles apportent d'importants changements aux politiques et procédures actuelles.

Aux termes de l'article 13 de la *Loi sur la protection des renseignements personnels et les documents électroniques,* je suis autorisé à demander aux organisations de faire rapport sur les progrès réalisés pour mettre en œuvre ces changements, et suivant l'expérience jusqu'à date, il s'agit d'une démarche utile qui permettra d'assurer que les changements nécessaires sont apportés.

La démarche que j'ai adoptée concernant les enquêtes et la résolution des plaintes ressemble à la démarche aux termes de la *Loi sur la protection des renseignements personnels*. Lorsqu'une plainte est déposée au Commissariat, j'avise officiellement l'organisation de la nature des allégations et je l'invite à présenter des observations. Dans la mesure du possible, j'essaie de régler les différends par la conciliation, la consultation, la persuasion et la médiation.

Je peux rendre l'une des conclusions suivantes dans le traitement d'une plainte :

- **Non fondée :** Aucun élément de preuve n'a été relevé qui me porte à conclure que l'organisation a violé la *Loi*.
- **Fondée :** L'enquête a permis d'établir que l'organisation n'a pas respecté une disposition de la *Loi*.
- **Résolue :** L'organisation a pris des mesures correctives pour remédier à la situation, ou le plaignant est satisfait des résultats de l'enquête du Commissariat.
- **Abandonnée :** Il s'agit d'enquêtes qui ont pris fin avant que toutes les allégations aient été pleinement examinées. Une affaire peut être abandonnée pour un nombre de raisons, par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire.

Les Conclusions du Commissaire

Voici mes conclusions aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques* jusqu'au 30 novembre 2001. À des fins d'uniformité, les conclusions sont présentées dans le format tel qu'elles apparaîtront sur notre site Web à **www.privcom.gc.ca** . Depuis janvier 2001, le Commissariat a entrepris des enquêtes et rendu des conclusions ainsi que des recommandations d'enquêtes sur 27 plaintes aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques*, et deux incidents. Les plaintes de nature presque identique ont été groupées et une seule conclusion a été rendue.

Activités de surveillance vidéo dans un endroit public [principe énoncé à l'article 4.3 de l'annexe 1]

Plainte

Le Commissaire à l'information et à la vie privée des Territoires du Nord-Ouest et du Nunavut s'est plaint qu'une entreprise de services de sécurité ait indûment recueilli des renseignements personnels, sans le consentement des individus visés, en ayant recours à des caméras de surveillance installées dans la rue principale de Yellowknife.

Résumé de l'enquête

L'entreprise de services de sécurité en question avait installé, sur le toit de l'édifice de ses bureaux, quatre caméras vidéos braquées sur la principale intersection de Yellowknife, de même que deux moniteurs dans ses bureaux. Au début de mai 2001, le personnel de l'entreprise a surveillé pendant plusieurs jours des images en direct, jour et nuit. À plusieurs reprises, le personnel de l'entreprise a remarqué des délits et a communiqué avec le service de police. De l'aveu de l'entreprise, ses activités de surveillance faisaient partie d'un projet de marketing qui visait à stimuler les affaires. Vu la publicité négative que le projet a suscité, l'entreprise a retiré ses caméras moins d'une semaine après les avoir installées.

Conclusions du Commissaire (rendues le 15 juin 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que toute entreprise dans les Territoires du Nord-Ouest est une entreprise fédérale au sens de la *Loi.*

Application : Le principe énoncé à l'article 4.3 de l'annexe 1 précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

Le Commissaire a conclu que puisque la surveillance des faits et gestes du public constituait le principal objectif de l'installation de l'équipement de surveillance vidéo, les renseignements en cause étaient considérés comme personnels aux termes de la *Loi.* L'entreprise ayant admis que ses activités de surveillance vidéo relevaient d'un projet de marketing, le Commissaire a conclu qu'il s'agissait d'une activité commerciale au sens de la *Loi.*

Le fait que l'image vidéo était transmise en direct et n'était pas enregistrée a été jugé non pertinent puisqu'au regard de la *Loi,* les renseignements personnels ne se limitent pas aux seuls renseignements enregistrés. En se fondant sur les preuves, le Commissaire était d'avis que les individus n'avaient pas consenti à la collecte. Il a conclu que l'entreprise avait recueilli des renseignements personnels sans le consentement des intéressés au mépris du principe énoncé à l'article 4.3.

Au moment de présenter ses conclusions, le Commissaire a formulé les commentaires suivants : [traduction] « Il peut arriver qu'il soit approprié de surveiller des endroits publics pour des raisons de sécurité publique. Il faut toutefois limiter cette pratique aux seuls cas où il est possible d'en démontrer le besoin. Il faut que seules les autorités publiques légitimes puissent effectuer ces activités, et seulement d'une façon qui tienne compte toutes les mesures de protection de

la vie privée prévues dans la *Loi*. Dans notre société, la surveillance non autorisée des endroits publics, à des fins commerciales, par des organisations du secteur privé n'a pas sa place. »

Le Commissaire a donc conclu que la plainte était fondée.

Autres considérations

Il n'était pas nécessaire de prendre d'autres mesures à l'égard de la plainte, puisque l'entreprise avait déjà retiré les caméras avant que le Commissaire ait rendu ses conclusions. Néanmoins, l'affaire n'était pas tout à fait réglée, du fait que l'entreprise de services de sécurité avait signalé qu'elle avait l'intention de continuer de déployer des efforts dans le but d'offrir des services de surveillance vidéo aux membres de la communauté de Yellowknife. Le Commissaire a indiqué à l'entreprise que son projet de surveillance vidéo du public à des fins commerciales est illégal et qu'elle devait l'abandonner.

Messages électroniques non sollicités d'un fournisseur de services Internet [principe énoncé à l'article 4.3 de l'annexe 1]

Plainte

Une cliente s'est plainte que son fournisseur de services Internet (FSI), en lui envoyant des communications électroniques non sollicitées, ait utilisé sans son consentement des renseignements personnels la concernant, à savoir son adresse électronique.

Résumé de l'enquête

Le FSI de la plaignante lui avait fait parvenir plusieurs messages électroniques non sollicités portant sur ses services. Tout d'abord, elle s'est plainte directement auprès du FSI, mais la suggestion de l'entreprise, qui l'a invitée tout simplement à reconfigurer son fureteur de façon que les messages soient envoyés directement dans un sous-répertoire de courrier en vrac ou dans la corbeille, ne l'a pas satisfaite. Elle soutenait que l'utilisateur ne devrait pas porter le fardeau de déceler les communications électroniques non sollicitées du FSI. Pour sa part, l'entreprise soutenait qu'elle était en droit d'envoyer de tels messages, en vertu des modalités et conditions de l'entente d'abonnement, qui comprend une clause de consentement.

La plaignante, dont le premier abonnement d'un an était un cadeau d'un ami, n'avait pas étudié personnellement ces modalités et conditions au départ, mais en a pris connaissance par la suite, au renouvellement de son abonnement après la première année. La plaignante a renouvelé son abonnement auprès de la même entreprise même si à ce moment-là, sa plainte n'était toujours pas réglée.

Conclusions du Commissaire (rendues le 3 juillet 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les fournisseurs de services Internet sont des entreprises fédérales au sens de la *Loi.*

Application : Le principe énoncé à l'article 4.3 de l'annexe 1 précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

Après avoir examiné l'entente d'abonnement du FSI en question, le Commissaire était d'avis que la pratique d'envoi de communications électroniques périodiques à la clientèle était décrite clairement dans l'entente. Par conséquent, il a jugé qu'il était raisonnable que les clients s'attendent à recevoir, de temps à autre, de pareilles communications. De plus, il a considéré que la plaignante avait consenti à cette pratique en renouvelant son abonnement. Il a conclu que dans cette affaire, le FSI n'avait pas contrevenu au principe énoncé à l'article 4.3.

Le Commissaire a donc conclu que la plainte n'était pas fondée.

Autres considérations

Le Commissaire a signalé à la plaignante qu'il estimait que la première suggestion formulée par le FSI en vue de résoudre son problème était raisonnable.

Il a en outre formulé le commentaire suivant : [traduction] « Les communications électroniques sont conformes avec l'objet du consentement d'utilisation de l'adresse électronique qui, à l'origine, avait été obtenu pour permettre la prestation efficace des services du FSI. »

Le Commissaire étudie le domaine de compétence dans une affaire de communication de renseignements d'une filiale bancaire à un tiers [article 30]

Plainte

Un client s'est plaint qu'une société de placement, filiale d'une banque à charte, ait indûment communiqué à un tiers, c'est-à-dire à l'organisme de réglementation qui surveille les activités de la société, des renseignements personnels relatifs à ses opérations financières.

Résumé de l'enquête

Dans cette affaire, le Commissaire devait déterminer si la plainte relevait ou non de ses compétences.

Conclusions du Commissaire (rendues le 19 juillet 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique strictement aux entreprises fédérales et aux communications de renseignements personnels pour contrepartie à l'extérieur

d'une province. Les banques sont des entreprises fédérales au sens de la *Loi*. Toutefois, dans la présente affaire, encore que la société de placement soit une filiale bancaire, elle est exploitée en tant que personne morale, elle ne communique pas de renseignements pour contrepartie à l'extérieur de la province, et elle est sous réglementation provinciale. À l'heure actuelle, la société en question n'est pas visée par la *Loi*.

Le Commissaire a conclu qu'il n'était pas de son ressort de faire enquête sur cette plainte.

Une cliente d'une banque demande des renseignements sur sa cote de crédit [principe énoncé à l'article 4.9 de l'annexe 1, et article 8]

Plainte

Une cliente s'est plainte qu'une banque ne lui ait pas permis de consulter ses renseignements personnels concernant sa cote de crédit.

Résumé de l'enquête

La plaignante avait téléphoné à la succursale de la banque en question pour demander des renseignements au sujet de sa cote de crédit. Un représentant du service à la clientèle de la succursale lui a répondu que la banque ne divulguait pas ces renseignements à ses clients. La banque, ayant appris le dépôt de cette plainte, a entrepris une recherche approfondie dans ses dossiers et a signalé par la suite qu'il ne s'y trouvait pas d'entente ou de demande de crédit au nom de la plaignante, et que par conséquent, la banque ne disposait pas de cote de crédit pour cette cliente. La plaignante a confirmé subséquemment qu'elle n'avait pas conclu d'entente de crédit avec cette banque, à laquelle elle n'avait par ailleurs jamais présenté de demande de crédit.

Conclusions du Commissaire (rendues le 23 juillet 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les établissements financiers sont des entreprises fédérales au sens de la *Loi*.

Application : Le principe énoncé à l'article 4.9 de l'annexe 1 précise qu'une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'utilisation qui en est faite et de leur communication à des tiers, et lui permettre de les consulter. L'article 8 établit les conditions en fonction desquelles une organisation serait réputée avoir refusé d'acquiescer à la demande.

Le Commissaire était convaincu que les dossiers de la banque ne contenaient pas les renseignements que la plaignante avait demandés. Il a donc conclu que la banque n'avait pas privé la plaignante de son droit de consulter les renseignements personnels qui la concernent en vertu de l'article 8 de la *Loi*.

Le Commissaire a conclu que la plainte n'était pas fondée.

Conservation de renseignements personnels après le rejet d'une demande [principe énoncé à l'article 4.5 de l'annexe 1]

Plainte

Une particulière qui avait présenté une demande de carte de crédit s'est plainte que la banque, après l'avoir rejetée, ait refusé de satisfaire à sa requête pour que les renseignements personnels recueillis dans sa demande soient supprimés des dossiers de la banque.

Résumé de l'enquête

La plaignante avait présenté en personne une demande de carte de crédit, mais la banque en question l'avait rejetée. La plaignante a ensuite demandé que les renseignements personnels qu'elle avait inscrits dans sa demande soient retirés du système informatique de la banque. Le directeur de la succursale a répondu que le pouvoir de supprimer des renseignements ne lui avait pas été délégué, et il n'a pas tenté d'établir s'il était possible d'entreprendre d'autres démarches à cette fin.

De fait, l'agent de protection de la vie privée et le gestionnaire des opérations des cartes de crédit étaient investis par délégation du pouvoir de retirer ces renseignements sur demande spéciale, mais dans la présente affaire, la demande de la plaignante n'a pas été transmise à l'un ou l'autre de ces responsables. À la banque, la pratique courante relative aux demandes de carte de crédit présentées en personne consistait à saisir immédiatement les renseignements personnels dans le système informatique de la succursale, puis de les envoyer au système hôte du centre d'évaluation des dossiers de financement pour soumettre la demande à la décision de la banque. Si la demande était refusée, les renseignements n'étaient pas éliminés automatiquement. Sauf sur demande spéciale de l'individu dont la demande avait été rejetée, les renseignements personnels le concernant étaient conservés dans le système informatique de la banque, où le personnel de la succursale pouvait y avoir accès indéfiniment.

Conclusions du Commissaire (rendues le 23 juillet 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les banques sont des entreprises fédérales au sens de la *Loi*.

Application : Le principe énoncé à l'article 4.5 de l'annexe 1 stipule que les renseignements personnels doivent être conservés aussi longtemps que nécessaire pour la réalisation des fins auxquelles ils ont été recueillis.

Le Commissaire a jugé déraisonnable le fait que si la plaignante n'avait pas insisté pour qu'ils soient retirés, les renseignements personnels la concernant auraient pu demeurer

accessibles indéfinitivement à la succursale, après que la banque les a utilisés pour des fins auxquelles ils avaient été recueillis (c.-à-d. la prise de décision au sujet de la carte de crédit). Il a conclu que dans cette affaire, la banque avait contrevenu au principe énoncé à l'article 4.5.

Néanmoins, le Commissaire a également fait observer que la banque avait, par la suite, supprimé les renseignements personnels concernant la plaignante et confirmé qu'ils n'avaient pas été communiqués à un tiers. En outre, il a signalé que le plaignante était satisfaite de ce règlement.

Le Commissaire a donc conclu que la plainte était fondée et résolue.

Autres considérations

En vue d'aborder les irrégularités décelées dans l'enquête du Commissaire, la banque en question a convenu d'entreprendre un examen approfondi de ses pratiques courantes de conservation des renseignements personnels. La banque a également convenu de mettre en œuvre une stratégie de communication visant à informer les employés et les clients de sa procédure relative aux plaintes concernant la protection des renseignements personnels.

Sûreté du service téléphonique automatisé d'une banque [principe énoncé à l'article 4.7 de l'annexe 1]

Plainte

Invoquant plusieurs dispositions de la *Loi sur la protection des renseignements personnels et les documents électroniques*, un individu s'est plaint qu'une banque n'ait pas appliqué les mesures de sécurité convenables pour protéger les renseignements concernant la clientèle qui sont communiqués au moyen de son service téléphonique automatisé.

Résumé de l'enquête

La banque en question offre un service téléphonique automatisé aux titulaires de cartes Visa qui ne font pas d'autres opérations auprès de cette banque. Les utilisateurs de ce service ne peuvent faire de transactions mais peuvent consulter certains renseignements relatifs à leur compte Visa en composant les 16 chiffres de leur numéro de compte et, suivant le choix au hasard du système, les quatre derniers chiffres du numéro de téléphone à domicile ou l'année de naissance du titulaire de la carte.

Conclusions du Commissaire (rendues le 23 juillet 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette

plainte était du ressort du Commissaire parce que les banques sont des entreprises fédérales au sens de la *Loi*.

Application : Le principe énoncé à l'article 4.7 de l'annexe 1 précise que les renseignements personnels doivent être protégés par une organisation au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

Après avoir examiné la plainte, le Commissaire a jugé la préoccupation du plaignant valable. Il a établi qu'un processus de codage reposant à un point tel sur le numéro de téléphone ou l'année de naissance du titulaire de la carte ne suffisait pas à empêcher des personnes non autorisées de consulter des renseignements personnels à caractère délicat concernant les utilisateurs. Il a jugé que la banque n'était pas en conformité avec le principe énoncé à l'article 4.7.

Néanmoins, le Commissaire a observé que la banque avait proposé et entrepris un plan d'action détaillé en trois étapes visant à régler les problèmes de sécurité soulevés dans la plainte. En outre, il a observé que le plaignant et lui-même ont jugé tous les aspects du plan satisfaisants.

Le Commissaire a donc conclu que la plainte était fondée et résolue.

Autres considérations
Le plan d'action proposé par la banque comprend les trois étapes suivantes :

Immédiat : L'accès automatisé au compte Visa du plaignant est bloqué, de sorte que toute tentative non autorisée de consultation des renseignements personnels du plaignant échouera. Le plaignant pourra lui-même consulter son compte par l'intermédiaire d'un mandataire, au moyen d'un mot de passe préétabli.

À court terme : D'ici le 31 octobre 2001, les clients de Visa qui ne font pas d'autres opérations auprès de cette banque pourront bloquer l'accès téléphonique automatisé à leur compte sur demande et pourront, s'ils le souhaitent, transiger directement avec un mandataire. Cette étape comprend une stratégie de communication visant à informer les clients à ce sujet.

À long terme : La banque a convenu de mettre en œuvre, au cours des trois prochaines années, un nouveau service bancaire téléphonique qui remédiera aux préoccupations des clients quant à la protection de la vie privée et à la sûreté du service, et de rendre compte des progrès accomplis au Commissaire à la protection de la vie privée au plus tard le 31 juillet 2002.

Le Commissaire a formulé le commentaire suivant : [traduction] « Je suis d'avis que les mesures que [la banque] a prises pour résoudre les problèmes de sûreté soulevés … sont acceptables. »

Un musicien s'oppose à ce qu'une organisation professionnelle recueille des renseignements sur son salaire [article 2]

Plainte

Un musicien s'est plaint que l'organisation professionnelle chargée de représenter ses intérêts ait, sans son consentement, recueilli des renseignements personnels à son sujet, à savoir son salaire annuel, auprès de son employeur.

Résumé de l'enquête

Le plaignant est le seul musicien à l'emploi d'un certain établissement. L'organisation professionnelle en question doit, au nombre de ses activités, recueillir les droits d'auteur pour ses membres, conformément aux exigences de la *Loi sur le droit d'auteur*. En vue de produire le tarif applicable auprès de la Commission du droit d'auteur et de percevoir les redevances, l'organisation doit déterminer avant tout le budget global de divertissement d'un établissement donné. La préoccupation du plaignant venait du fait que puisqu'il était le seul musicien à l'emploi de l'établissement en question, un tiers aurait pu le reconnaître comme seul bénéficiaire de l'affectation réservée aux salaires dans le budget de divertissement. Toutefois, l'identification des musiciens ou la détermination du nombre de musiciens travaillant dans un établissement ne présument pas d'intérêt pour l'organisation dans la collecte de tels renseignements, et c'est pourquoi elle ne recueille pas de noms ou de nombres. En outre, l'organisation ne publie pas et ne communique pas à des tiers les renseignements qu'elle recueille au sujet de l'établissement.

Conclusions du Commissaire (rendues le 23 juillet 2001)

Compétence : L'organisation professionnelle en question a affirmé qu'elle était visée par la *Loi sur la protection des renseignements personnels et les documents électroniques*. Le Commissaire n'a pas contesté cette position.

Application : Selon l'article 2 de la *Loi*, un renseignement personnel se dit de « [...] tout renseignement concernant un individu identifiable [...] ».

En se fondant sur les preuves, le Commissaire était d'avis que l'organisation professionnelle était autorisée par la *Loi* à recueillir les renseignements en cause et que la collecte ne portait pas sur des renseignements personnels concernant un individu identifiable. Par conséquent, il a conclu que la collecte n'était donc pas visée par les dispositions de la *Loi*.

Le Commissaire a conclu que la plainte n'était pas fondée.

Autres considérations

Au moment de communiquer ses conclusions, le Commissaire a formulé le commentaire suivant : [traduction] « Puisque j'ai établi que les renseignements recueillis ne sont pas personnels, j'ai jugé que je n'ai pas besoin de poser de conclusions quant à leur

bien-fondé en considération des articles 4.3 (consentement) et 4.4 (limitation de la collecte) de l'annexe 1 et de l'article 7 (collecte à l'insu de l'intéressé et sans son consentement) de la *Loi*, qui, autrement, auraient pu s'appliquer à la présente plainte. »

Utilisation et communication de renseignements personnels dans les annuaires téléphoniques [principe énoncé à l'article 4.3 de l'annexe 1]

Plainte

Invoquant plusieurs dispositions de la *Loi sur la protection des renseignements personnels et les documents électroniques*, un particulier s'est plaint qu'une entreprise de télécommunications :

1. ait utilisé et communiqué des renseignements personnels concernant les clients à leur insu et sans avoir obtenu leur consentement, en publiant leur nom, leur adresse et leurs numéros de téléphone dans les pages blanches de l'entreprise et sur deux sites Web; et
2. ait indûment exigé des clients qu'ils paient pour ne pas publier les renseignements personnels qui les concernent.

Résumé de l'enquête

L'entreprise de télécommunications en question publie les nom, adresse et numéros de téléphone de ses clients dans ses pages blanches et sur son propre site Web d'assistance-annuaire. Conformément aux règlements du CRTC, l'entreprise transmet ces renseignements à la filiale de Bell Canada qui exploite du site Web « Canada 411 ». Les clients sont invités à préciser la façon dont ils souhaitent que les renseignements personnels les concernant figurent dans les pages blanches de l'entreprise et peuvent demander que ces renseignements ne soient pas publiés. L'entreprise exige des frais de service aux clients qui demandent la non-publication, conformément aux règlements du CRTC. En outre, l'entreprise, moyennant frais, fournit à certaines organisations des services de listes qui ne comprennent pas de renseignements sur les clients qui ont choisi la non-publication et sur les clients qui demandent que leur nom soit rayé.

Conclusions du Commissaire (rendues le 14 août 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les entreprises de télécommunications sont tenues pour des entreprises fédérales au sens de la *Loi*.

Application : Le principe énoncé à l'article 4.3 de l'annexe 1 précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

Au sujet du consentement, le Commissaire a jugé que la question que l'entreprise posait à ses clients quant à la façon dont les renseignements les concernant devraient figurer dans les pages blanches était pertinente. Il a établi que la question implique en soi la publication éventuelle des renseignements dans des annuaires auxquels le public a accès. Les clients qui choisissent de ne pas se prévaloir de l'option de non-publication consentent implicitement à ce que des renseignements personnels les concernant deviennent accessibles au public. De plus, puisque les renseignements publiés par la suite sur d'autres supports correspondent tout à fait à ceux qui sont publiés dans les pages blanches, pour l'application des règlements en vertu de la *Loi*, ils sont également tenus pour des renseignements auxquels le public a accès et il est possible de les recueillir, de les utiliser et de les communiquer sans le consentement de la personne concernée. En somme, le Commissaire a conclu que l'entreprise avait obtenu un consentement valable et observait les règlements sur les renseignements auxquels le public a accès.

Au sujet des frais exigés pour la non-publication des renseignements concernant les clients, le Commissaire a constaté que l'entreprise avait dûment demandé la permission du CRTC, qui la lui avait accordée, en vertu de l'Ordonnance Télécom 98-109, qui stipule que les sociétés de télécommunications peuvent exiger jusqu'à au plus 2 $ par mois pour un service de numéro non publié. Par conséquent, il a conclu que l'entreprise en cause était habilitée à exiger son tarif mensuel de non-publication établi à 2 $.

Le Commissaire a conclu que la plainte n'était pas fondée.

Inscription du numéro de compte sur un chèque à la banque [paragraphe 5(3)]

Plainte

Un individu s'est plaint qu'une banque ait créé un risque de communication inappropriée à un tiers de renseignements personnels le concernant, sans son consentement, lorsqu'un caissier a inscrit son numéro de compte à l'endos d'un chèque au moment de l'encaissement.

Résumé de l'enquête

Le plaignant avait visité une succursale de sa banque pour encaisser un chèque personnel d'un tiers. Le caissier a inscrit le numéro de compte du plaignant à l'endos du chèque. La préoccupation du plaignant tenait au fait que s'il fallait retourner le chèque au tiré pour quelque raison que ce soit, son numéro de compte serait divulgué à cette personne.

La banque a fait valoir que lorsqu'elle encaisse des chèques, elle accorde un crédit jusqu'à ce que la valeur du chèque puisse être portée au débit du compte du tiré. Dans des cas

exceptionnels (p. ex. fraude ou insuffisance de provision), la banque doit pouvoir recourir à un moyen efficace pour récupérer la somme du chèque auprès du client qui l'a encaissé. À cette fin, les noms inscrits au verso des chèques ne constituent pas un moyen suffisamment efficace, car ils peuvent différer pour la peine des noms exacts sous lesquels les comptes bancaires des clients sont ouverts. La banque a soutenu que l'inscription des numéros de compte sur les chèques est une pratique de longue date dans toute l'industrie, et qu'il faut l'appliquer pour protéger les intérêts de la banque en veillant à ce qu'elle puisse percevoir les sommes auprès du tiré ou les récupérer auprès de la personne qui dépose ou encaisse le chèque.

Conclusions du Commissaire (rendues le 14 août 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les banques sont des entreprises fédérales au sens de la *Loi*.

Application : Le paragraphe 5(3) prévoit que l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Le Commissaire a établi que la pratique bancaire qui consiste à inscrire le numéro de compte sur le chèque au moment de l'encaissement est raisonnable et qu'il est raisonnable qu'un client s'attende à ce qu'il en soit ainsi. Le Commissaire était d'avis que le plaignant avait donc consenti implicitement à la collecte, à l'utilisation et à la communication de renseignements personnels qui le concernent. Le Commissaire a conclu qu'il n'avait pas été établi que cette pratique contrevenait à la *Loi*.

Il a donc conclu que la plainte n'était pas fondée.

Autres considérations

Au moment de présenter ses conclusions, le Commissaire a formulé le commentaire suivant : [traduction] « Lorsqu'il remet un chèque pour l'encaisser, le client de la banque donne son consentement implicite à la communication des renseignements personnels qui figurent à l'endos du chèque, au même titre que le tiré donne son consentement explicite à la communication des renseignements personnels le concernant (qui figurent au verso du chèque) au tireur. »

Une entreprise de camionnage recueille des renseignements personnels prévus pour Douanes Canada [principe énoncé à l'article 4.4 de l'annexe 1]

Plainte

Un employé licencié s'est plaint que son ancien employeur, entreprise internationale de camionnage, ait indûment tenté de recueillir des renseignements personnels à son sujet car elle a insisté pour qu'il remplisse et lui renvoie une formule de demande pour un programme établi par l'Agence des douanes et du revenu du Canada (ADRC).

Résumé de l'enquête

L'entreprise de camionnage en question avait envoyé au plaignant, l'un de ses conducteurs internationaux, une lettre indiquant qu'il devait remplir une « demande de participation au programme d'inscription des chauffeurs du secteur commercial » dans le cadre du nouveau Programme d'autocotisation des douanes établi par l'ADRC. La lettre indiquait également que le conducteur devait renvoyer la demande remplie à l'entreprise. Le plaignant a refusé, souhaitant éviter que son employeur ne puisse consulter les renseignements personnels qu'il devait inscrire sur la formule. L'entreprise lui a fait parvenir une seconde lettre qui l'ordonnait au plaignant de remplir et de renvoyer la demande avant une certaine date, sans quoi il ferait l'objet de mesures disciplinaires en vertu de l'entente collective, et son emploi serait compromis. De nouveau, le plaignant n'a pas accédé à cette demande, et l'entreprise a mis fin à son emploi cinq jours après la date indiquée. Aux dires de l'entreprise, l'ADRC attendait des employeurs qu'ils recueillent les demandes et les remettent à l'ADRC pour le compte des conducteurs. De fait, l'ADRC indique clairement, tant sur la formule de demande que dans la brochure portant sur le programme, que les conducteurs doivent remettre leur demande remplie directement au centre de traitement de l'ADRC, à Niagara Falls.

Conclusions du Commissaire (rendues le 17 août 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les entreprises interprovinciales de camionnage sont des entreprises fédérales au sens de la *Loi*.

Application : Le principe énoncé à l'article 4.4 de l'annexe 1 stipule que l'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et qu'elle doit le faire de façon honnête et licite.

Le Commissaire a établi que, bien que les conducteurs remplissent une demande pour le Programme d'autocotisation des douanes et la renvoyer à l'ADRC, il n'était pas nécessaire ou approprié que l'entreprise recueille elle-même les renseignements. De plus, il a établi qu'il n'était pas honnête de menacer les employés de les relever de leurs fonctions dans le but de recueillir les renseignements. Il a jugé que l'entreprise n'était pas conforme au principe énoncé à l'article 4.4.

Le Commissaire a observé que l'entreprise avait modifié rapidement sa politique afin que les conducteurs ne soient plus tenus de renvoyer leur demande à l'entreprise. Il n'estimait toutefois pas que la plainte était réglée car que l'employé devait réintégrer dans l'entreprise et qu'il obtienne réparation. Le Commissaire a signalé qu'il avait l'intention de donner suite à cette plainte auprès de l'entreprise.

Le Commissaire a conclu que la plainte était fondée.

Autres considérations

Le plaignant a subséquemment informé le Commissaire qu'un règlement au sujet de son congédiement était intervenu par arbitrage et que pour ce motif, il estimait que la plainte avait été réglée de façon satisfaisante.

Une banque perd des renseignements personnels concernant une cliente [principe énoncé à l'article 4.7 de l'annexe 1, et paragraphe 12(2)]

Plainte

Une cliente s'est plainte qu'une banque ait manqué de protéger des renseignements personnels la concernant lorsque des documents contenant ses numéro d'assurance sociale (NAS), nom, adresse et numéro de téléphone non inscrit à l'annuaire ont été perdus au cours d'un transfert d'un bureau à l'autre.

Résumé de l'enquête

Développement des ressources humaines Canada avait remis un nouveau numéro d'assurance sociale à la plaignante après qu'elle eut découvert que le précédent avait été utilisé frauduleusement. Plus tard, elle a rempli des formules dont la banque avait besoin pour modifier avec son nouveau NAS des renseignements concernant son compte de placement. Elle a remis les formules remplies au personnel d'une succursale locale de la banque afin qu'elles soient transmises au bureau de la succursale où le compte de placement est administré. Les documents ont été perdus au cours du transfert.

Conclusions du Commissaire (rendues le 7 septembre 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les banques sont des entreprises fédérales au sens de la *Loi*.

Application : Le principe énoncé à l'article 4.7 de l'annexe 1 précise que les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. Le paragraphe 12(2) stipule que le Commissaire peut tenter de parvenir au règlement de la plainte en ayant recours à un mode de règlement des différends, notamment la médiation et la conciliation.

Dans l'enquête du Commissaire, les parties se sont montrées intéressées dès le départ à régler la plainte. Il s'en est suivi une discussion jusqu'à ce qu'intervienne, en fin de compte, un règlement à la satisfaction des deux parties. De plus, le Commissaire était d'avis que la banque en question avait pris des mesures afin de s'assurer que les politiques, pratiques et procédures appropriées de protection étaient en place.

Le Commissaire a donc conclu que la plainte était réglée et qu'il n'était pas nécessaire de prendre d'autres mesures.

Autres considérations

La plaignante et la banque se sont estimées satisfaites du rôle joué par le Commissariat dans le règlement de cette plainte.

Un demandeur de carte de crédit s'oppose à la politique sur l'échange de renseignements d'une banque

Plainte

Un individu s'est plaint qu'une banque ait refusé de traiter sa demande de carte de crédit parce qu'il ne voulait pas consentir à la politique sur l'échange de renseignements de la banque.

Résumé de l'enquête

En remplissant une demande de carte de crédit, le plaignant en a modifié à la main les modalités et conditions. Il espérait exprimer de la sorte son désaccord quant à la politique sur l'échange de renseignements personnels de la banque et exercer son droit de refuser que des renseignements personnels qui le concernent soient communiqués et de refuser de recevoir les services de marketing direct de la banque. La banque lui a envoyé par la suite une lettre qui indiquait qu'il lui était impossible de traiter sa demande telle quelle parce que le libellé avait été modifié. Le plaignant a compris que la lettre indiquait que la banque refusait de lui accorder une carte de crédit à moins qu'il ne consente à sa politique sur l'échange de renseignements. Dans une deuxième lettre, la banque a indiqué au

plaignant que les demandeurs étaient en droit de choisir de ne pas recevoir les services de marketing direct, et que sa propre demande lui avait été renvoyée tout simplement parce qu'il l'avait modifiée. De plus, la banque a offert au plaignant d'examiner de nouveau sa demande de carte de crédit et, du même coup, de rayer son nom des listes de marketing direct et de marketing croisé. Le plaignant a accepté cette offre.

Le plaignant, qui s'est finalement vu accorder une carte de crédit, s'est déclaré satisfait du suivi de la banque et a indiqué que son dossier de plainte auprès du Commissariat à la protection de la vie privée pouvait être fermé.

Par conséquent, cette plainte a été abandonnée.

Une banque accusée de retenir des certificats d'obligation [principe énoncé à l'article 4.9 de l'annexe 1, et article 8]

Plainte

Une particulière s'est plainte qu'une banque ait refusé qu'elle consulte des renseignements personnels la concernant, à savoir deux « obligations pour la petite entreprise », immatriculées à son nom, qu'elle croyait que la banque détenait.

Résumé de l'enquête

La plaignante a précisé que les documents qu'elle demandait étaient deux « obligations pour la petite entreprise » sur support papier ou sous forme de certificats. En 1982, la plaignante et son conjoint avaient consolidé leurs dettes existantes à la banque en question dans le cadre du Programme des obligations des petites entreprises, initiative fédérale qui accordait une exemption d'intérêts aux emprunteurs. Dès 1984, la banque avait signalé à la plaignante que « l'obligation pour la petite entreprise » n'était qu'une expression et que le seul véritable document dûment signé ayant trait au Programme des obligations des petites entreprises était la formule intitulée « Choix commun à l'égard d'une obligation pour le développement de la petite entreprise ». La banque et Industrie Canada ont confirmé que cette formule était le seul document directement relié au programme. Il n'y avait jamais eu d'obligations pour la petite entreprise sur support papier ou sous forme de certificats. En 1998, au cours d'une poursuite relative à la défaillance de la plaignante à l'égard de son contrat de prêt, la banque avait dû remettre à la plaignante et à son avocat tous les documents relatifs à sa participation au Programme des obligations des petites entreprises qu'elle détenait. La plaignante avait alors reçu sa formule dûment signée de « Choix commun à l'égard d'une obligation pour le développement de la petite entreprise », qu'elle avait toujours en sa possession lorsqu'elle a déposé sa plainte auprès du Commissariat à la protection de la vie privée.

Conclusions du Commissaire (rendues le 18 septembre 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les banques sont des entreprises fédérales au sens de la *Loi.*

Application : Le principe énoncé à l'article 4.9 de l'annexe 1 précise qu'une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'utilisation de leur communication à des tiers, et lui permettre de les consulter. L'article 8 établit les conditions en fonction desquelles une organisation serait réputée avoir refusé d'acquiescer à la demande.

Le Commissaire n'a relevé aucun élément de preuve démontrant l'existence de documents concernant les obligations pour la petite entreprise, hormis celui que la plaignante avait déjà reçu. Convaincu que les documents que demandait la plaignante n'existaient pas, le Commissaire a conclu que la banque n'avait pas privé la plaignante de son droit de les consulter.

Le Commissaire a donc conclu que la plainte n'était pas fondée.

Vente de renseignements sur les habitudes de prescription des médecins [articles 2 et 3]

Deux Plaintes

Dans deux plaintes distinctes un individu et un médecin se sont plaints qu'une branche canadienne d'une entreprise internationale de marketing des États-Unis ait indûment communiqué des renseignements personnels en recueillant et en vendant des données relatives aux habitudes de prescription des médecins sans leur consentement.

Résumé de l'enquête

L'entreprise de marketing en question recueille, auprès de pharmacies et d'autres sources canadiennes, des données relatives aux ordonnances médicales. Les renseignements réunis comprennent des noms, des numéros d'identité, des numéros de téléphone et des particularités de prescription des médecins. Ces renseignements sont transmis au centre de traitement des données de l'entreprise aux États-Unis, où l'entreprise produit des produits d'information personnalisés. Ces produits, en général, dressent une liste des médecins d'un certain territoire et les classent, individuellement ou en groupes, suivant leur activité mensuelle de prescription de divers types ou diverses catégories de médicaments. Ces produits d'information sont ensuite transférés à l'établissement de Montréal, où ils sont communiqués aux clients, moyennant

frais. Les représentants en produits pharmaceutiques de plusieurs provinces canadiennes achètent régulièrement ces produits.

Conclusions du Commissaire (rendues le 21 septembre 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique à toute communication de renseignements personnels pour contrepartie à l'extérieur d'une province. Puisque les renseignements en cause étaient régulièrement communiqués à l'extérieur de la province, le Commissaire a établi qu'il s'agissait de communications de renseignements pour contrepartie à l'extérieur d'une province et par conséquent, il était tenu de recevoir cette plainte et de faire enquête.

Application : Selon l'article 2 de la *Loi*, un renseignement personnel se dit de « tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail ». L'article 3 de la *Loi* expose l'objet de la *Loi*, qui consiste à établir un équilibre entre le droit des individus à la vie privée et le besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables.

Le Commissaire devait déterminer avant tout si les renseignements en cause étaient des renseignements personnels au sens et selon la portée et l'objet de la *Loi*. Dans cette question, le sens de « renseignement personnel », bien que vaste, ne l'est pas assez pour englober tous les renseignements associés à un individu, de l'avis du Commissaire. L'ordonnance individuelle, quoiqu'elle puisse révéler des renseignements au sujet du patient, n'est pas, de façon significative, un renseignement concernant le médecin prescripteur comme individu. Il s'agit plutôt d'un renseignement concernant le processus professionnel qui a débouché sur sa délivrance, et il faudrait considérer que l'ordonnance est un produit de travail, c'est-à-dire le résultat tangible de l'activité professionnelle du médecin.

Le Commissaire a établi qu'une interprétation de « renseignement personnel » qui serait assez vaste pour englober les ordonnances ou les habitudes de prescription ne permettrait pas de réaliser l'objet exposé à l'article 3 de la *Loi* (voir ci-dessus). Plus précisément, il ne serait pas raisonnable d'élargir la définition pour englober les ordonnances, de crainte qu'elle ne s'applique en outre à tous les autres produits de travail, comme les avis juridiques ou les documents rédigés dans le cadre du travail. Il apparaît qu'il n'est pas plus raisonnable d'élargir la définition pour englober les habitudes de prescription, de crainte qu'elle

ne s'applique en outre aux habitudes que permettraient de découvrir d'autres genres de produits de travail, et par conséquent, que de nombreux genres de rapports commerciaux légitimes pour les consommateurs ne soient interdits.

En somme, le Commissaire a conclu que les renseignements sur les ordonnances, que ce soit sous forme d'ordonnances individuelles ou sous forme de tendances dégagées d'un certain nombre d'ordonnances, ne sont pas des renseignements personnels concernant un médecin.

Le Commissaire a donc conclu que les plaintes n'étaient pas fondées.

Autres considérations

En raison de l'intérêt général que cette plainte a suscité auprès du public, le Commissaire a publié sa lettre de conclusions sous forme de communiqué, le 2 octobre 2001.

Obstacles à la démarche d'un exécuteur testamentaire tâchant d'obtenir des renseignements concernant un coffre bancaire [principes énoncés aux articles 4.5 et 4.9 de l'annexe 1, et paragraphe 8(7)]

Plainte

Un exécuteur testamentaire s'est plaint qu'une banque ait refusé d'acquiescer à sa demande de renseignements personnels concernant le coffre bancaire de sa tante décédée.

Résumé de l'enquête

Le plaignant soupçonnait qu'une certaine personne non autorisée avait, avec le concours des avocats de la succession, accédé au coffre bancaire de la tante décédée et pris des articles de valeur. Le plaignant avait recueilli un élément de preuve (c-à-d une réponse négative d'une succursale de la banque ayant été transmise par télécopieur) qui évoquait fortement la possibilité que la banque ait reçu des avocats au moins une demande indépendante se rapportant au portefeuille bancaire de la défunte. En sa qualité d'exécuteur testamentaire, le plaignant a demandé à la banque de consulter la carte de signatures pour le coffre bancaire et toute correspondance entre la banque et les avocats de la succession. La banque a répondu qu'il lui était impossible de trouver la carte ou les éléments de correspondance. La recherche approfondie dans les dossiers bancaires, qu'ont menée l'ombudsman de la banque, l'Ombudsman bancaire canadien et le Commissariat à la protection de la vie privée, n'a pas permis de trouver les renseignements demandés par le plaignant.

En temps normal, la banque conserve les cartes de signatures subordonnées aux coffres bancaires pendant sept ans. Huit jours après le décès de la tante, tous les coffres bancaires avaient été transférés d'une succursale bancaire à une autre, et les mesures de sécurité qui s'imposent avaient été appliquées au cours du transfert. La politique bancaire ne

prévoyait pas, toutefois, qu'une succursale conserve des dossiers sur un compte, un placement ou un coffre bancaire après leur transfert dans une autre succursale. La politique bancaire ne prévoyait pas plus qu'une succursale conserve des demandes de renseignements relatifs à un dossier qui ne s'y trouvait plus.

Conclusions du Commissaire (rendues le 12 octobre 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les banques sont des entreprises fédérales au sens de la *Loi*.

Application : Le principe énoncé à l'article 4.9 de l'annexe 1 précise qu'une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'utilisation et de leur communication à des tiers, et lui permettre de les consulter. Le paragraphe 8(7) précise que l'organisation qui refuse, dans le délai prévu, d'acquiescer à la demande notifie par écrit au demandeur son refus motivé et l'informe des recours que lui accorde la présente partie.

Le Commissaire a établi que les renseignements que la banque n'a pu produire auraient dû être conservés conformément au principe énoncé à l'article 4.5, et n'auraient pas dû être perdus. Par conséquent, il a jugé que la banque n'avait pas respecté le principe énoncé à l'article 4.9. Il a en outre jugé que la réponse de la banque constituait un refus aux termes du paragraphe 8(7).

Le Commissaire a donc conclu que la plainte était fondée.

Autres considérations

Le Commissaire a recommandé que la banque révise ses pratiques relatives à la destruction des documents contenant des renseignements personnels et élabore une politique écrite portant sur la conservation de tels documents, conformément aux dispositions pertinentes de la *Loi*.

Un employé prétend que son employeur a communiqué sans son consentement des renseignements à une société de placement [paragraphe 7(3) et principes énoncés aux articles 4.3 et 4.5 de l'annexe 1]

Plainte

Un employé d'une grande entreprise s'est plaint que son employeur ait indûment communiqué des renseignements personnels le concernant et concernant d'autres employés, y compris de l'information relative aux primes en espèce, sans avoir obtenu le consentement des employés ou les en avoir informés au préalable, à une société de placement qui s'occupe d'un REER et d'un régime d'épargne offerts par l'entreprise.

Résumé de l'enquête

L'entreprise en question a reconnu qu'elle communique des renseignements personnels concernant ses employés, sans avoir obtenu leur consentement explicite, à la société de placement qui s'occupe du REER et du régime d'épargne pour les employés à salaire horaire. Les renseignements divulgués comprennent les numéros de registre de paie et d'identité personnelle, nom, adresse, numéro d'assurance sociale, état matrimonial, sexe, langue de prédilection, date d'entrée en fonction, date de naissance, service, code de groupe et code syndical de l'individu. En outre, l'entreprise avertit la société de placement lorsqu'elle attribue des primes en espèce, sans toutefois préciser le nom du bénéficiaire ou le montant de la prime. Le REER et le régime d'épargne ont été établis par l'entreprise en vue de respecter l'engagement passé avec le syndicat du personnel en vertu de la convention collective. L'entreprise paie la société de placement pour les services fournis dans le cadre du régime et ne communique pas de renseignements à la société de placement pour contrepartie, qu'elle soit monétaire ou autre.

Conclusions du Commissaire (rendues le 18 octobre 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique strictement aux entreprises fédérales et aux communications de renseignements personnels pour contrepartie à l'extérieur d'une province. L'entreprise en question n'est pas une entreprise fédérale au sens de la *Loi*, et elle ne communique pas les renseignements personnels en cause à l'extérieur de la province pour contrepartie.

Le Commissaire a conclu qu'il n'était pas de son ressort de poursuivre l'enquête sur cette plainte.

Un demandeur affirme ne pas avoir reçu son rapport de solvabilité d'une agence d'évaluation [article 8]

Plainte

Un individu s'est plaint qu'une agence d'évaluation du crédit ait refusé d'acquiescer à sa demande de consulter son rapport de solvabilité.

Résumé de l'enquête

Le plaignant avait écrit à l'agence d'évaluation du crédit pour demander de consulter tout rapport de solvabilité le concernant que l'agence aurait conservé dans ses dossiers. Dans sa plainte, il a affirmé ne pas avoir reçu, par la suite, de réponse de l'agence. Le centre des relations avec la clientèle de l'agence compte six employés qui sont chargés de recevoir et de traiter les demandes d'accès conformément aux formalités établies. Suivant ces formalités, une demande d'un client n'est pas classée avant d'avoir été assortie à un rapport de solvabilité ayant été envoyé par la poste ou remis au client. La demande d'accès du plaignant, qui porte une note manuscrite

indiquant qu'une réponse a été envoyée à l'adresse exacte du plaignant 13 jours après la réception de sa demande, se trouve dans les dossiers du centre. Le dépôt de la réponse à la poste était également confirmé par renvoi à un registre informatisé et à un rapport de vérification établi par ordinateur. Le plaignant, à un moment donné, a admis qu'il était possible qu'il ait tout simplement négligé de remarquer le rapport de solvabilité lorsqu'il l'a reçu. Il a déclaré ultérieurement qu'il était fort improbable qu'il ait reçu le rapport sans le remarquer.

Conclusions du Commissaire (rendues le 26 octobre 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique à toute communication de renseignements personnels pour contrepartie à l'extérieur d'une province. Cette plainte était du ressort du Commissaire parce que l'agence d'évaluation du crédit en question avait communiqué des renseignements personnels pour contrepartie à l'extérieur de la province.

Application : Le paragraphe 8(3) de la *Loi* précise que l'organisation saisie de la demande doit y donner suite avec la diligence voulue et, en tout état de cause, dans les trente jours suivant sa réception. Le paragraphe 8(5) précise que faute de répondre dans le délai, l'organisation est réputée avoir refusé d'acquiescer à la demande.

Le Commissaire n'a pas relevé de motif pour mettre en doute les éléments de preuve qui démontraient que l'agence d'évaluation du crédit avait reçu la demande d'accès du plaignant et lui avait envoyé une réponse par la poste dans le délai de réponse prescrit. Il a conclu que l'agence avait observé le paragraphe 8(3) de la *Loi*.

Le Commissaire a conclu que la plainte n'était pas fondée en vertu du paragraphe 8(5).

Une entreprise de transport aérien accusée de priver des voyageurs de leur droit de consulter des renseignements personnels au sujet d'incidents de voyage [principes énoncés aux articles 4.1 et 4.9 de l'annexe 1]

Plainte

Trois voyageurs aériens se sont plaints qu'une entreprise de transport aérien les ait privés de leur droit de consulter des renseignements personnels concernant leurs expériences au cours d'un voyage au Mexique.

Résumé de l'enquête

Les plaignants avaient demandé de consulter tous les renseignements personnels relatifs à certains événements qu'ils avaient vécus au cours d'un voyage au Mexique que détenaient l'entreprise de transport aérien et les services de voyage associés. Dans un premier temps, un représentant a répondu que l'entreprise n'était pas tenue de produire ces renseignements. Après que le Commissariat à la protection de la vie privée l'eut informée des

obligations auxquelles elle était liée en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, l'entreprise a aussitôt pris des mesures en vue de nommer un agent responsable de la conformité avec la *Loi*, a traité la demande d'accès des plaignants et leur a envoyé les renseignements personnels sur lesquels la demande portait. Les plaignants étaient d'avis, après avoir examiné ces renseignements, que l'entreprise n'avait pas joint les rapports d'incident. L'enquêteur pour le compte du Commissaire à la protection de la vie privée a examiné les dossiers originaux qui contenaient les renseignements personnels concernant les plaignants que détenait l'entreprise, mais rien n'indiquait qu'il existait des renseignements autres que ceux que les plaignants avaient déjà reçus. L'entreprise a confirmé par écrit qu'elle ne détenait pas d'autres renseignements au sujet des plaignants, y compris des rapports d'incident.

Conclusions du Commissaire (rendues le 31 octobre 2001)

Compétence : Depuis le 1er janvier 2001, la *LPRPDÉ* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les entreprises de transport aérien sont des entreprises fédérales au sens de la *Loi*.

Application : Le principe énoncé à l'article 4.1 de l'annexe 1 précise qu'une organisation est responsable des renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect [des principes stipulés à] l'annexe 1. Le principe énoncé à l'article 4.9 précise qu'une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'utilisation et de leur communication, à des tiers, et lui permettre de les consulter.

En ce qui concerne le principe énoncé à l'article 4.1, le Commissaire a établi que l'entreprise de transport aérien n'avait pas désigné de responsable avant l'intervention du Commissariat. Par conséquent, il a jugé que l'entreprise, au départ, ne respectait pas ce principe. Néanmoins, il a également observé que l'entreprise avait depuis nommé un agent supérieur chargé d'assurer la conformité avec la *Loi*. Le Commissaire a jugé que cette question était réglée.

En ce qui concerne le principe énoncé à l'article 4.9, le Commissaire a établi que de nouveau, l'entreprise n'avait remis aux plaignants les renseignements personnels les concernant qu'après l'intervention du Commissariat. Par conséquent, il a jugé que l'entreprise, au départ, ne respectait pas ce principe. Il a toutefois observé que les plaignants étaient convaincus d'avoir reçu tous les renseignements personnels les concernant que l'entreprise détenait. De plus, les plaignants étaient satisfaits du résultat de l'enquête.

Le Commissaire a conclu que la plainte était fondée et résolue.

Une employée s'oppose à ce que son employeur inscrive son numéro de compte bancaire sur sa fiche de paie [principes énoncés aux articles 4.3 et 4.7 de l'annexe 1]

Plainte

Une employée d'une entreprise de télécommunications s'est plainte que son employeur :

1. ait utilisé des renseignements personnels la concernant à une fin à laquelle elle n'avait pas consenti en imprimant ses numéros de compte bancaire de domiciliation de la banque sur sa fiche de paie; et

2. n'ait pas protégé convenablement les fiches de paie du personnel, compte tenu du degré de sensibilité des renseignements qu'elles contiennent.

Résumé de l'enquête

Les employés de l'entreprise de télécommunications en question reçoivent leur paie par virement automatique, et leurs fiches de paie leur sont remises sous pli cacheté dans leur milieu de travail. En raison d'une fusion et de la conversion subséquente des systèmes de rémunération, les numéros de compte bancaire et de domiciliation de la banque sont inscrits sur les fiches de paie de tous les employés depuis le 1er janvier 2001. L'impression de ces numéros sur les fiches de paie est devenue pratique courante dans les secteurs privé et public. Sur les fiches produites par cette entreprise, rien n'indique ce que désignent les numéros, et seules les personnes qui connaissent bien les codes d'information de la banque sauraient ce qu'ils représentent. Les enveloppes cachetées contenant les fiches de rémunération du personnel, lorsqu'elles sont livrées au milieu de travail de la plaignante, sont réunies dans une plus grande enveloppe qui est déposée sur le bureau du gestionnaire, où il arrive souvent, au cours de périodes comptant jusqu'à 24 heures, qu'elle soit laissée à découvert et sans surveillance.

À l'origine, la plaignante avait consenti à ce que sa paie soit déposée directement dans son compte bancaire, mais elle n'a jamais donné son consentement explicite pour que ces numéros figurent sur sa fiche. C'est pourquoi elle a affirmé que son employeur utilisait des renseignements personnels concernant son compte bancaire sans son consentement et à une fin qui n'était pas compatible avec celle à laquelle elle avait fourni les renseignements au départ. De plus, elle a affirmé que son employeur ne protégeait pas convenablement les fiches de paie du personnel dans son milieu de travail.

L'entreprise a soutenu que les renseignements étaient bel et bien utilisés à la seule fin à laquelle ils avaient été recueillis, à savoir le virement automatique des paies; qu'il était désormais impératif, pour les besoins de la vérification de l'affectation des fonds salariaux et la résolution des écarts, d'imprimer les numéros de compte et de succursale sur les fiches de paie; et que bon nombre d'employés en étaient déjà venus à s'attendre à ce que ces

numéros soient inscrits sur leur fiche, et à s'y fier. De plus, l'entreprise a soutenu avoir protégé convenablement les renseignements relatifs aux comptes bancaires de ses employés, car elle distribuait les fiches sous pli confidentiel et cacheté.

Conclusions du Commissaire (rendues le 5 novembre 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les entreprises de télécommunications sont des entreprises fédérales au sens de la *Loi*.

Application : Le principe énoncé à l'article 4.3 de l'annexe 1 précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire. Ce principe stipule en outre (à l'article 4.3.5) que les attentes raisonnables de la personne sont pertinentes. Le principe énoncé à l'article 4.7 précise que les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

Au sujet du premier élément de la plainte (consentement), le Commissaire a établi qu'il était raisonnable que les employés qui divulguent leurs numéros de compte bancaire et de domiciliation de la banque aux fins du virement automatique s'attendent à ce que ces numéros figurent sur les fiches de transaction aux fins de la vérification de l'affectation des fonds, lesquelles correspondent tout à fait aux fins convenues. Il était donc d'avis que la plaignante avait donné son consentement implicite. Par conséquent, il a jugé que l'entreprise avait satisfait à ses obligations en vertu du principe énoncé à l'article 4.3 de l'annexe 1.

Le Commissaire a conclu qu'à cet égard, la plainte n'était pas fondée.

Au sujet du deuxième élément de la plainte (mesures de sécurité), le Commissaire a établi que les mesures de contrôle opérationnel appliquées par l'entreprise dans le milieu de travail de la plaignante ne correspondaient pas au degré de sensibilité des renseignements personnels contenus dans les fiches de paie. Il a jugé que l'entreprise avait manqué à ses obligations en vertu du principe énoncé à l'article 4.7 de l'annexe 1.

Il a toutefois observé que l'entreprise, après qu'elle eut été informée de ses obligations, avait pris immédiatement des mesures appropriées pour corriger ses pratiques de gestion de l'information relativement aux fiches de paie du personnel.

Le Commissaire a conclu qu'à cet égard, la plainte était fondée et résolue.

Autres considérations

L'entreprise a convenu de mettre en œuvre, comme solution à court terme, des mesures de contrôle opérationnel plus rigoureuses dans le milieu de travail de la plaignante et d'offrir à la plaignante la possibilité de recevoir sa fiche de paie par la poste, à domicile.

Une entreprise demande le NAS d'une cliente en vertu d'une politique [principes énoncés aux articles 4.3.3 et 4.4.1 de l'annexe 1, et paragraphe 5(3)]

Plainte

Une particulière s'est plainte qu'une entreprise de télécommunications ait indûment recueilli des renseignements personnels la concernant, à savoir son numéro d'assurance sociale (NAS).

Résumé de l'enquête

L'entreprise de télécommunications en question avait demandé le NAS de la plaignante au moment de la conclusion d'une entente de service de connexion Internet avec elle. Aux dires de la plaignante, le représentant de l'entreprise avec qui elle s'était entretenue lui avait signifié que « sans NAS, pas de connexion », de sorte qu'elle s'était sentie obligée de donner son numéro pour recevoir le service. La collecte du NAS des clients éventuels était prévue par la politique écrite de l'entreprise. Cette politique visait à éviter que des similarités dans les noms des clients ne prêtent à confusion. Néanmoins, selon cette politique, l'entreprise ne devait pas insister pour connaître le NAS des clients qui refusaient de le divulguer, et l'entreprise avait signalé à son personnel que la collecte n'était pas obligatoire.

Conclusions du Commissaire (rendues le 5 novembre 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les entreprises de télécommunications sont des entreprises fédérales au sens de la *Loi*.

Application : Le principe énoncé à l'article 4.3.3 de l'annexe 1 précise qu'une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées. Le principe énoncé à l'article 4.4.1 précise que les organisations ne doivent pas recueillir des renseignements de façon arbitraire. On doit restreindre tant la quantité que la nature des renseignements recueillis à ce qui est nécessaire pour réaliser les fins déterminées. Le paragraphe 5(3) stipule que l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

En ce qui concerne le principe énoncé à l'article 4.4.1, le Commissaire a établi que, conformément à la politique de l'entreprise, la collecte des NAS n'était pas obligatoire et que, pour ce motif, elle n'était pas nécessaire pour réaliser les fins légitimes et explicitement indiquées. Par conséquent, il a jugé que la collecte était arbitraire et que l'entreprise contrevenait à ce principe.

En ce qui concerne le principe énoncé à l'article 4.3.3, le Commissaire était d'avis qu'on avait nettement donné l'impression à la plaignante que la divulgation de son NAS était une condition du service. Par conséquent, il a jugé que l'entreprise contrevenait à ce principe.

En ce qui concerne le paragraphe 5(3), le Commissaire s'est penché attentivement sur une position défendue depuis longtemps au Commissariat, selon laquelle il ne faudrait pas recourir au NAS comme à un identificateur universel et les citoyens ne devraient pas divulguer leur NAS à moins que la loi ne les y oblige pour la réalisation des fins d'un certain nombre de programmes fédéraux qui sont en droit de recueillir ces renseignements. Il était d'avis qu'une personne raisonnable s'opposerait à la collecte de NAS pour un service de connexion Internet. Par conséquent, il a jugé que l'entreprise contrevenait aux dispositions du paragraphe 5(3).

Le Commissaire a observé que l'entreprise avait supprimé le NAS en cause du dossier de la plaignante et qu'elle en était à modifier sa politique afin que les NAS ne soient plus demandés.

Le Commissaire a donc conclu que la plainte était fondée et résolue.

Autres considérations

Le Commissaire a également recommandé que l'entreprise mette en œuvre une démarche d'examen de ses dossiers et qu'elle supprime tous les autres NAS ayant été inutilement recueillis auprès de ses clients.

Une utilisatrice accuse un FSI de lire ses messages électroniques et d'empêcher leur transmission [principe énoncé à l'article 4.3 de l'annexe 1]

Plainte

Une particulière s'est plainte que son ancien fournisseur de services Internet (FSI) :

1. ait indûment recueilli des renseignements personnels la concernant, sans son consentement, du fait qu'il ait lu ses messages électroniques; et
2. ait empêché la transmission de messages électroniques qu'elle tentait d'envoyer à des utilisateurs de son ancien FSI par le biais d'un nouveau FSI.

Résumé de l'enquête

La plaignante avait été abonnée aux services d'un certain FSI pendant deux ans. Au cours de cette période, son utilisation du compte, et plus particulièrement, ses tentatives de transmission de fichiers volumineux par courrier électronique, avaient provoqué un conflit entre elle et le FSI. Elle a affirmé que le fournisseur lui avait alors dit pouvoir lire ses messages électroniques. Elle a en outre affirmé qu'après qu'elle eut déménagé dans une autre ville et souscrit un abonnement auprès d'un autre FSI, ce même fournisseur avait commencé à bloquer la transmission de messages électroniques qu'elle tentait de faire parvenir à des utilisateurs de son ancien FSI. Le fournisseur en question a déclaré qu'il ne se souvenait pas de s'être trouvé en désaccord avec la plaignante, mais il a admis que selon la pratique courante, à la découverte d'un grand nombre de messages « d'échec de remise » (signalant les tentatives de transmission de fichiers volumineux par courrier électronique), il aurait appelé l'utilisateur en cause afin de discuter de la question. Il a nié pouvoir lire des messages liés au compte de la plaignante à part ceux qui indiquent un « échec de remise ». Il a aussi nié avoir empêché la transmission des messages de la plaignante.

L'enquête a confirmé que le FSI en question peut surveiller les activités relatives aux comptes des utilisateurs et déceler les messages « d'échec de remise », mais qu'il ne reçoit pas de messages électroniques ou de pièces jointes et ne peut pas lire les messages électroniques des utilisateurs. En outre, il n'y avait pas d'élément de preuve indiquant que le fournisseur avait empêché la transmission des messages électroniques de la plaignante par son nouveau serveur. De fait, plusieurs semaines avant que le fournisseur ne soit avisé de la plainte déposée contre lui, le problème de transmission a cessé lorsqu'un technicien en informatique a modifié l'adresse IP de l'ordinateur de la plaignante.

Conclusions du Commissaire (rendues le 5 novembre 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les fournisseurs de services Internet sont des entreprises fédérales au sens de la *Loi*.

Application : Le principe énoncé à l'article 4.3 de l'annexe 1 précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

Le Commissaire était d'avis qu'il aurait été impossible au FSI de lire les messages électroniques de ses utilisateurs, et que le FSI n'avait pas empêché la transmission des messages de la plaignante. De plus, il a établi qu'une personne raisonnable s'attendrait à ce que le FSI surveille les services qu'il fournit et donne suite à des messages récurrents « d'échec de remise ». Il a conclu que dans cette affaire, le FSI ne contrevenait pas au principe énoncé à l'article 4.3 de l'annexe 1.

Le Commissaire a donc conclu que la plainte n'était pas fondée.

Un employeur envoie à des tiers des copies d'une réponse à des demandes d'accès présentées par une employée [principes énoncés aux articles 4.3 et 4.5 de l'annexe 1, et paragraphe 5(3)]

Plainte

Une employée d'une administration aéroportuaire s'est plainte que son employeur ait, sans son consentement, communiqué à des tiers des renseignements personnels la concernant en leur envoyant des copies d'une lettre de réponse à des demandes d'accès qu'elle avait présentées.

Résumé de l'enquête

La plaignante avait présenté des demandes d'accès, en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, afin de consulter des renseignements que détenait son employeur.

L'employeur lui a par la suite envoyé une lettre de réponse qui indiquait que l'organisation rejetait ses demandes. La lettre indiquait en outre que des copies de la réponse seraient adressées à trois autres personnes : deux représentants syndicaux et le coordonnateur des relations avec les employés de l'aéroport. La plaignante n'avait pas fait parvenir de copies de ses demandes d'accès à ces parties et n'avait pas consenti explicitement à ce que des copies de la lettre de réponse leur soient envoyées.

Les représentants syndicaux avaient précédemment participé à une réunion au cours de laquelle la question de l'accès aux renseignements personnels concernant la plaignante avait été soulevée. Le coordonnateur des relations avec les employés était précédemment intervenu dans une plainte de harcèlement déposée par la même plaignante et il détenait certains des documents connexes qu'elle demandait à consulter. L'employeur a fait valoir que la plaignante avait donné son consentement implicite à la communication de ces renseignements à ces personnes suivant les motifs de ces interventions antérieures. La plaignante a soutenu qu'elle avait présenté les demandes d'accès personnellement et en son propre nom, sans le concours du syndicat.

Conclusions du Commissaire (rendues le 5 novembre 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les aéroports sont des entreprises fédérales au sens de la *Loi.*

Application : Le principe énoncé à l'article 4.3 de l'annexe 1 précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire. Le principe énoncé à l'article 4.5 stipule que les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. Le paragraphe 5(3) précise que l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

En ce qui concerne le principe énoncé à l'article 4.3 et la communication des renseignements aux représentants syndicaux, le Commissaire a établi que l'employeur aurait été autorisé par consentement implicite à envoyer les copies de la réponse à ces parties seulement si la plaignante avait indiqué qu'elle leur avait fait parvenir des copies de ses demandes d'accès. La plaignante était en droit d'exercer son recours officiel sans le concours du syndicat, et l'employeur n'était pas tenu d'informer le syndicat de sa réponse. Il a conclu qu'il n'y avait pas eu de consentement implicite se rapportant aux représentants syndicaux. En ce qui concerne le paragraphe 5(3), le Commissaire était d'avis qu'une personne raisonnable aurait estimé que la communication des renseignements aux représentants syndicaux était inacceptable.

Il a donc conclu que cet aspect de la plainte était fondé.

En ce qui concerne le principe énoncé à l'article 4.5 et le coordonnateur des relations avec les employés, compte tenu de la participation directe de cette personne dans la demande d'accès, le Commissaire a établi qu'il était approprié que l'employeur informe le coordonnateur de sa décision de refuser d'acquiescer à la demande d'accès à des documents présentée par la plaignante. En ce qui concerne le paragraphe 5(3), le Commissaire était d'avis qu'une personne raisonnable aurait estimé que la communication des renseignements au coordonnateur des relations avec les employés était acceptable.

Il a conclu que l'employeur s'est conformé au principe énoncé à l'article 4.5 concernant la question du coordinateur des relations avec les employés.

Il a donc conclu que cet aspect de la plainte n'était pas fondé.

Autres considérations

Au cours de l'enquête, le Commissariat à la protection de la vie privée a signalé à l'administration aéroportuaire en question qu'il est préférable de ne pas faire parvenir à des tiers des copies des réponses et qu'il faut plutôt laisser le soin à chaque demandeur de déterminer s'il souhaite faire connaître ces réponses à d'autres personnes après l'avoir reçue. Le Commissaire s'est réjoui de constater que l'organisation avait suivi ses conseils pour traiter des demandes d'accès présentées subséquemment par la plaignante.

Une entreprise de téléphone demande des pièces d'identité aux nouveaux abonnés [principes énoncés aux articles 4.2 et 4.2.3 et aux articles 4.3, 4.3.2 et 4.3.3 de l'annexe 1, et paragraphe 5(3)]

Plainte

Une particulière s'est plainte qu'une entreprise de télécommunications ait indûment recueilli des renseignements personnels auprès de nouveaux abonnés en exigeant que ses nouveaux clients qui refusent de produire ces renseignements versent un acompte.

Résumé de l'enquête

Lorsque la plaignante a tenté de s'abonner à un nouveau service téléphonique auprès de l'entreprise en question, un téléphoniste lui a demandé de produire deux pièces d'identité. La plaignante s'est montrée hésitante, et le téléphoniste lui a dit que si elle refusait de le faire, elle devrait verser un acompte. Le téléphoniste lui a aussi dit que la collecte de ces renseignements visait à confirmer son identité. Le superviseur de l'entreprise lui a subséquemment expliqué la collecte de la même façon, et a confirmé qu'à défaut de produire ces renseignements, la plaignante devrait verser un acompte.

La politique de l'entreprise prévoit que les téléphonistes doivent demander aux nouveaux abonnés de produire deux pièces d'identité, exiger un acompte en cas de refus, et expliquer que la collecte de ces renseignements vise tout simplement à confirmer l'identité de l'abonné. Toutefois, lorsque le demandeur est un nouveau client qui n'a jamais fait affaire avec l'entreprise, la collecte a pour véritable objet de procéder à la vérification du crédit de cette personne, conformément aux règlements du CRTC, étant donné que l'entreprise, lorsqu'elle fournit des services téléphoniques, accorde un crédit à l'utilisateur.

Conclusions du Commissaire (rendues le 8 novembre 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les entreprises de télécommunications sont des entreprises fédérales au sens de la *Loi*.

Application : Le principe énoncé à l'article 4.2.3 stipule que les fins auxquelles les renseignements sont destinés doivent être précisées avant la collecte ou au moment de celle-ci. Le principe énoncé à l'article 4.3.2 précise que les organisations doivent faire un effort raisonnable pour informer la personne concernée des fins auxquelles les renseignements seront utilisés et pour énoncer les fins de façon que la personne puisse raisonnablement les comprendre. Le principe énoncé à l'article 4.3.3 stipule qu'une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que celles qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées. Le paragraphe 5(3) précise que l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

En ce qui concerne le principe énoncé à l'article 4.3.3 et le paragraphe 5(3), le Commissaire a établi qu'une personne raisonnable estimerait qu'il est acceptable que l'entreprise recueille des renseignements personnels pour les besoins de la confirmation de la solvabilité des clients éventuels ou, lorsqu'il s'agit de clients réguliers, de la confirmation de leur identité.

Il a conclu qu'à cet égard, la plainte n'était pas fondée.

En ce qui concerne les principes énoncés aux articles 4.2.3 et 4.3.2, le Commissaire a établi qu'une personne raisonnable conclurait que l'entreprise n'avait pas exposé explicitement l'objet de sa collecte de renseignements personnels concernant les nouveaux abonnés.

Il a conclu qu'à cet égard, la plainte était fondée.

Autres considérations

L'entreprise a convenu de modifier sa pratique et d'exposer les fins de la collecte. Plus particulièrement, l'entreprise avisera les nouveaux abonnés que la collecte de renseignements vise à évaluer leur solvabilité, étant donné que l'entreprise fait crédit à l'utilisateur lorsqu'elle lui fournit un service interurbain.

Un radiodiffuseur accusé de recueillir des renseignements personnels sur son site Web [article 2, et principe énoncé à l'article 4.3 de l'annexe 1]

Plainte

Un particulier s'est plaint qu'un radiodiffuseur ait tenté de recueillir, au moyen de son serveur publicitaire, des renseignements personnels qui le concernent, à savoir l'information NetBIOS de son ordinateur, sans avoir obtenu son consentement.

Résumé de l'enquête

Le plaignant avait un ordinateur équipé d'un modem câble pour la connexion Internet et d'un garde-barrière pour la détection et le rejet des tentatives d'intrusion. Chaque fois que le plaignant essayait d'entrer en communication avec le site Web de l'organisation, son garde-barrière détectait et rejetait une démarche de collecte de l'information NetBIOS de son ordinateur lancée par le serveur publicitaire de l'organisation, puis produisait un rapport à ce sujet. NetBIOS est le nom courant ou « convivial » désignant un ordinateur suivant à son adresse IP.

Le dépistage d'une adresse IP permet d'avoir accès à des renseignements comme les sites Web qu'a visités l'utilisateur de l'ordinateur ou les mots de passe qu'il a utilisés récemment pour consulter des comptes protégés. Lorsqu'un utilisateur a accès à Internet par réseau commuté, la probabilité que l'adresse IP de son ordinateur soit dépistée est faible, mais celle-ci est beaucoup plus élevée si l'utilisateur a une connexion Internet permanente par modem câble, comme dans le cas du plaignant.

Après avoir mené des enquêtes à l'interne, le radiodiffuseur a ajouté foi à la prétention du plaignant. Le radiodiffuseur a expliqué que le gestionnaire de réseau, au moment d'installer Windows NT de Microsoft, avait négligé de désactiver certaines caractéristiques qui accompagnent le programme. Lorsque ces caractéristiques, qu'on appelle service WINS, sont en fonction, le serveur peut recueillir l'information NetBIOS des utilisateurs du site Web. Le gestionnaire du réseau, après avoir appris que les caractéristiques étaient en fonction, les a désactivées sans tarder. Le plaignant a confirmé par la suite que son garde-barrière ne relevait plus de tentative de collecte de l'information NetBIOS attribuable par l'organisation.

Conclusions du Commissaire (rendues le 20 novembre 2001)

Compétence : Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique aux entreprises fédérales. Cette plainte était du ressort du Commissaire parce que les radiodiffuseurs sont des entreprises fédérales au sens de la *Loi*.

Application : Selon l'article 2 de la *Loi*, un renseignement personnel se dit de « […] tout renseignement concernant un individu identifiable […] » Le principe énoncé à l'article 4.3 de l'annexe 1 précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

Le Commissaire était d'avis que dans certaines circonstances, comme la situation du plaignant, l'information NetBIOS peut servir à recueillir des renseignements qui peuvent être liés à un individu identifiable. Il a donc établi que les renseignements en cause étaient considérés comme personnels aux fins de la *Loi*.

Le Commissaire a conclu que le radiodiffuseur avait manqué à ses obligations en vertu du principe énoncé à l'article 4.3. Il n'a toutefois pas contesté l'explication de l'organisation selon laquelle le manquement était involontaire, il a fait observer qu'il avait pris des mesures satisfaisantes.

Il a donc conclu que la plainte était fondée et résolue.

Un couple prétend que la banque lui a refusé l'accès à des renseignements sur une demande de prêt [paragraphes 8(3) et 8(5)]

Deux plaintes

Un couple s'est plaint dans deux cas distincts qu'une banque leur ait refusé l'accès à des renseignements personnels le concernant, car elle n'a pas répondu à une demande d'information relative à une demande de prêt.

Résumé de l'enquête

Les plaignants avaient rédigé et présenté deux lettres, portant leur signature, pour demander des renseignements personnels relatifs à deux produits de crédit distincts qu'offrait la succursale locale de la banque en question. Les lettres étaient presque identiques, seules les lignes de mention objet les distinguaient, l'une indiquant un numéro de demande de prêt et l'autre, un numéro de prêt hypothécaire, toutes deux concernaient les deux plaignants. Au cours du mois suivant, la banque leur a fait parvenir les renseignements qu'ils avaient demandés au sujet de leur prêt hypothécaire, mais pas ceux ayant trait à leur demande de prêt. Les plaignants ont envoyé à la banque une autre lettre qui décrivait plus en détail les renseignements qu'ils voulaient obtenir au sujet de leur demande de prêt. Environ un mois après la soumission de la deuxième lettre, un avocat de la banque a

répondu aux plaignants en leur indiquant seulement qu'ils devraient couvrir les frais de photocopie, à raison de 25 cents la page. Les plaignants ont alors envoyé une autre lettre, à laquelle ils ont joint un chèque au montant des frais de photocopie, qui confirmait qu'ils souhaitaient toujours obtenir les renseignements demandés. Trois semaines après l'envoi de la lettre, ils n'avaient toujours pas reçu de réponse, et ils ont déposé une plainte auprès du Commissariat à la protection de la vie privée.

La banque a d'abord nié l'allégation, soutenant que la deuxième demande des plaignants était la première qui traitait de la demande de prêt. Toutefois, après qu'on lui ait présenté une copie de la première lettre portant sur la demande de prêt, la banque a vérifié ses dossiers puis a reconnu l'avoir reçue. La banque a expliqué qu'elle n'avait pas délibérément choisi de ne pas répondre à cette demande, mais que l'employé qui avait reçu la première lettre, n'avait pas relevé les lignes de mention objet différentes des deux lettres, et avait tenu pour acquis qu'elles étaient identiques. C'est pourquoi l'employé n'avait fait suivre que l'une des lettres (celle traitant du prêt hypothécaire).

Conclusions du Commissaire (rendues le 26 novembre 2001)

Compétence : Depuis le 1er janvier 2001, les entreprises fédérales tombent sous le coup de la *Loi sur la protection des renseignements personnels et les documents électroniques.* Cette plainte était du ressort du Commissaire parce que les banques sont des entreprises fédérales au sens de la *Loi.*

Application : Le paragraphe 8(3) de la *Loi* porte ce qui suit que l'organisation saisie de la demande doit y donner suite avec la diligence voulue et, en tout état de cause, dans les trente jours suivant sa réception. Le paragraphe 8(5) précise que faute de répondre dans le délai, l'organisation est réputée avoir refusé d'acquiescer à la demande.

Le Commissaire a conclu que la banque n'avait pas répondu dans le délai et contrevenait par conséquent à l'article 8. Il était toutefois d'avis que ce manquement était involontaire, et il a observé que par la suite, la banque avait fourni aux plaignants tous les renseignements visés par leur demande.

Il a donc conclu que les plaintes étaient fondées et résolues.

Incidents en vertu de la *LPRPDÉ*

Les incidents sont des affaires qui sont portées à mon attention par diverses sources, notamment des questions soulevées dans les médias. Il s'agit habituellement de situations dans lesquelles aucune victime n'a été identifiée et pour lesquelles aucune plainte n'a été déposée. Au cours des onze derniers mois, le Commissariat s'est penché sur les deux incidents suivants.

Une entreprise de transport recueille et communique des renseignements personnels concernant les passagers

Incident

On a prétendu que les agents de vente d'une compagnie de transport :

1. demandaient aux individus qui faisaient des réservations de billets de train au téléphone ou en personne pour le trajet Toronto-New York de divulguer leur date de naissance, leur citoyenneté et leur nom;
2. et communiquaient ces renseignements au Service des douanes américaines et au Service d'immigration et de naturalisation des États-Unis.

Résumé de l'enquête

L'entreprise a confirmé que la pratique en question avait lieu depuis décembre 2000, suivant une entente conclue entre l'entreprise de transport américaine, l'Agence canadienne des douanes et du revenu, et le Service des douanes américaines et le Service d'immigration et de naturalisation des États-Unis. Cette pratique vise à écourter l'attente à la frontière canado-américaine. De plus, les renseignements personnels recueillis à cette fin sont stockés dans le système informatique de réservation de l'entreprise et en sont supprimés si l'individu, finalement, n'achète pas de billet. Lorsque le passager achète de billet, ses nom, date de naissance et citoyenneté sont imprimés sur un manifeste, qui est ensuite transmis par télécopieur au Service des douanes américaines et au Service d'immigration et de naturalisation des États-Unis, et dont une copie est remise au directeur des services à bord du train. Le directeur des services détruit le manifeste peu après la fin du voyage.

Le Commissariat à la protection de la vie privée du Canada a établi que les agents de vente, à la demande écrite de l'entreprise, avaient présenté cette pratique comme une exigence à laquelle les passagers du trajet Toronto-New York devaient satisfaire.

Résultat

L'entreprise a demandé conseil au Commissariat à la protection de la vie privée du Canada quant à la façon de résoudre le problème de façon satisfaisante. Le Commissariat a recommandé à l'entreprise de communiquer à ses agents de vente des directives claires

selon lesquelles la communication de la date de naissance et de la citoyenneté est volontaire, et que les agents peuvent, après la réservation des billets, demander aux clients s'ils acceptent de divulguer ces renseignements en vue de faciliter les formalités douanières à la frontière.

Le Commissariat, après avoir reçu une copie des directives transmise par l'entreprise aux agents de vente, a informé l'entreprise que le dossier d'incident serait fermé, sous réserve de la surveillance continue des pratiques de réservation des agents de vente. En outre, le Commissariat a recommandé que l'entreprise envoie à tous ses agents, à un moment donné, une note de suivi établissant encore plus clairement qu'ils ne doivent pas recueillir de renseignements personnels au moment de la réservation sans le consentement éclairé de l'individu.

Un site Web diffuse des conversations par téléphones cellulaires

Incident

Le 7 juin 2001, le *Ottawa Sun* a publié un reportage selon lequel un site Web à Ottawa retransmettait sur Internet des conversations par téléphones cellulaires.

Un scanner interceptait des communications téléphoniques cellulaires. Il était relié à l'ordinateur hôte d'un site Web. Quiconque visitait le site Web pouvait écouter des conversations téléphoniques privées.

Résultat

Lorsque le Commissariat à la protection de la vie privée du Canada a lancé son enquête, le fournisseur de services Internet (FSI) en question a fermé le site Web en raison de problèmes de largeur de bande. Les problèmes étaient imputables à un employé qui, ayant son propre compte de réseau, transmettait des données par un autre serveur. Lorsqu'il a découvert ses activités, le FSI a immédiatement relevé l'employé de ses fonctions. Le FSI a indiqué que le site Web en question avait été transféré à un serveur de New York, sous une nouvelle direction.

Étant donné qu'on a fermé le site Web à Ottawa, l'enquête du Commissariat a été abandonnée. Le site Web sera surveillé périodiquement pendant une période indéterminée.

Genres d'enquête en vertu de la *LPRPDÉ*
1er janvier 2001 - 30 novembre 2001

Objet	Nombre
Dossiers criminels	30
Tests de dépistage de drogues	3
Chiffrement de données	7
Institutions fédérales	1 519
Vol d'identité	38
Demandes de renseignements	2 558
Interception – surveillance	154
Interprétation	2 024
Secteur de compétence	1 975
Marketing	439
Dossiers médicaux	137
Appels de députés	7
Demandes de publication	675
Numéro d'assurance sociale	1 834
Télécommunications	786
Transports	139
Autres	388
Total	12 713

Pratiques et examens en matière de vie privée

Aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques*, je suis autorisé à procéder à la vérification de la conformité des organisations privées dans la mesure où j'ai des « motifs raisonnables de croire » que celles-ci contreviennent à une disposition de la *Loi*.

Suivant les objectifs et les critères de vérification normalisés communément acceptés, la Direction des Examens et des pratiques en matière de vie privée du Commissariat effectue les examens et les vérifications de conformité aux termes de l'article 18 de la *Loi*. Comme la *Loi* n'est entrée en vigueur qu'au début de 2001, je n'ai toujours pas eu l'occasion d'effectuer de telle vérification. Mes efforts ont plutôt porté sur la sensibilisation des entreprises et des organisations à l'incidence de la nouvelle *Loi*, et j'ai tâché de leur donner des conseils pour qu'elles mettent en place des politiques en matière de vie privée qui soient conformes à la *Loi*.

Devant les tribunaux

Mathew Englander c. Telus Communications Inc.

Il s'agit de la première demande de révision judiciaire déposée devant la Cour fédérale en vertu de la *LPRPDÉ*. Le 1er janvier 2001, Mathew Englander a déposé une plainte auprès du Commissariat à la protection de la vie privée, dans laquelle il prétendait, entre autres choses, que Telus utilise et communique les nom, adresse et numéro de téléphone des consommateurs, à leur insu et sans leur consentement, pour les pages blanches de l'entreprise et à d'autres fins, et que Telus exige indûment des frais de service aux consommateurs qui choisissent la « non-publication » de leur numéro de téléphone. Selon le demandeur, ces mesures de Telus contreviennent aux paragraphes 5(1) et (3) de la *LPRPDÉ* et à plusieurs articles de l'annexe 1 de la *LPRPDÉ*.

Après avoir fait enquête sur la plainte, j'ai conclu que Telus est tout à fait conforme à la *Loi* concernant les motifs de la plainte, et qu'une personne raisonnable estimerait que Telus dans sa pratique d'initiation de service et la publication subséquente, dans les pages blanches de Telus, des renseignements personnels des consommateurs représentent une collecte, une utilisation et une communication indiquées de renseignements. J'ai en outre conclu que l'entreprise est autorisée à

exiger des frais à ses consommateurs pour un service de numéro non publié, et qu'il ne s'agit pas d'une pratique abusive qui contrevient au principe énoncé à l'article 4.3.3 de l'annexe 1.

Par conséquent, j'ai conclu que la plainte n'était pas fondée. M. Englander a demandé l'audition de la question devant la Cour, comme l'autorise l'article 14 de la *LPRPDÉ*.

Ronald G. Maheu c. le Procureur général du Canada et IMS Health Canada

Le demandeur a présenté une demande d'audition devant la Cour fédérale, comme l'autorise l'article 14 de la *LPRPDÉ*, après s'être plaint, auprès du Commissariat, que IMS Health ait communiqué à tort des renseignements personnels en recueillant et en vendant des données relatives aux habitudes de prescription des médecins sans leur consentement.

Après avoir fait enquête dans cette affaire, j'ai conclu que les renseignements sur les ordonnances, que ce soit sous forme d'ordonnances individuelles ou sous forme de tendances dégagées d'un certain nombre d'ordonnances, ne sont pas des renseignements personnels concernant un médecin. Touchant la question à savoir si les renseignements en cause étaient des renseignements personnels au sens et selon la portée et l'objet de la *Loi*, j'étais d'avis que le sens de « renseignement personnel », bien que vaste, ne l'est pas assez pour englober tous les renseignements associés à un individu. J'ai estimé que l'ordonnance individuelle, quoiqu'elle puisse révéler des renseignements au sujet d'un patient, n'est pas, de façon significative, un renseignement concernant le médecin prescripteur en tant qu'individu, mais qu'elle concerne plutôt le processus professionnel qui a débouché sur la délivrance de l'ordonnance, et qu'il faudrait considérer que l'ordonnance est un produit de travail, c'est-à-dire le résultat tangible de l'activité de travail du médecin. En somme, j'ai conclu que la plainte n'était pas fondée.

M. Maheu a présenté une demande d'audition devant la Cour. L'avis de demande comprenait une requête formulée par le demandeur, en vertu des règles de la Cour fédérale, pour que des documents détenus au Commissariat soient envoyés au demandeur et au Greffe de la Cour fédérale. Le Commissariat à la protection de la vie privée a refusé d'acquiescer à cette demande au motif que le Commissaire ne peut pas divulguer des documents qui ne sont pas déjà en la possession du demandeur, conformément aux dispositions de la *LPRPDÉ*.

Communications et sensibilisation du public

Aux termes de la *LPRPDÉ*, le Commissariat a été mandaté pour sensibiliser le public aux questions touchant la vie privée de façon à accroître sa connaissance et sa compréhension de ces questions. Pour donner suite à cette importante nouvelle responsabilité, l'établissement de la Direction des communications et des analyses stratégiques a été une des premières initiatives que j'ai entreprise suivant mon entrée en fonction. La Direction a réalisé un nombre d'activités l'an dernier pour sensibiliser davantage aux questions touchant la vie privée et pour renseigner les entreprises et les citoyens canadiens sur la nouvelle *Loi* visant le secteur privé.

L'art oratoire est un outil inestimable que j'emploie pour m'acquitter de mes responsabilités liées à la promotion et à la sensibilisation auprès du public concernant les questions de vie privée. J'ai prononcé 35 allocutions à un vaste éventail d'organisations partout au Canada et à l'étranger au cours de l'an dernier. Les cadres supérieurs du Commissariat ont prononcé 31 autres discours. Ces discours ont porté sur les principales questions d'actualité, comme la controverse entourant la sécurité et la vie privée qui a fait suite aux attaques du 11 septembre aux États-Unis. De nombreuses autres allocations ont présenté une occasion de renseigner les citoyens et les entreprises sur la nouvelle *Loi* et son incidence, de discuter de la vie privée en milieu de travail, et de faire part des préoccupations en matière de vie privée touchant des initiatives particulières, y compris Gouvernement en direct, les dossiers électroniques en matière de santé et l'usage accru de la surveillance vidéo.

De plus, en raison de l'influence exercée par les médias sur les sujets abordés lors de débats publics et de la sensibilisation accrue du public, le Commissariat a commencé à assurer un suivi proactif des questions touchant la vie privée abordées dans les médias, et je me suis davantage engagé dans diverses activités de relations avec les médias.

Ces activités comprennent des déclarations publiques, la diffusion de communiqués et d'articles de fond à la fois aux médias grand public et spécialisés; les entrevues avec les médias et la rencontre des comités de rédaction des médias et le soutien des relations avec les médias relativement aux discours, aux conférences et à d'autres événements spéciaux. De plus, le Commissariat répond à des demandes de renseignements des médias, faisant des observations et donnant des renseignements généraux touchant une vaste gamme de questions liées à la vie privée.

Le nombre de demandes de renseignements s'accroît tous les mois, et il est actuellement de 80 à 100 par mois en moyenne. En outre, j'ai accordé plus de 210 entrevues aux médias depuis septembre 2000.

Documents de sensibilisation du public

Le Commissariat a élaboré et diffusé des documents promotionnels et de sensibilisation en réponse à la grande demande de renseignements sur la *LPRPDÉ*. Nous avons publié des guides complets sur la nouvelle *Loi* à l'intention des entreprises et des individus. Plus de 21 000 exemplaires de ces deux guides ont été distribués au cours de l'année 2001.

De plus, nous avons conçu des affiches, des trousses en matière de vie privée, des bloc-notes et des signets. Tous ces documents répondent à la demande de renseignements sur les questions liées à la vie privée présentées par les individus, les entreprises et d'autres organisations.

Publicité

Dans le cadre du programme de rayonnement, qui vise à sensibiliser aux droits à la vie privée des Canadiens et Canadiennes dans le secteur privé concernant tout d'abord les entreprises réglementées par le fédéral, le Commissariat a fait paraître des publicités dans plus de 1 300 quotidiens et journaux communautaires dans toutes les régions du Canada. L'objet de ces publicités était de renseigner les Canadiens et les Canadiennes sur leurs droits aux termes de la *LPRPDÉ*. La campagne publicitaire, dont le thème était, *Your privacy is our concern – Votre vie privée, ça nous regarde*, qui a été diffusée en mars 2001, a joint des millions de Canadiens et Canadiennes dans tous les coins du pays.

Une deuxième publicité est parue dans 12 quotidiens sur les trois territoires, signalant que la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique à toutes les entreprises territoriales qui sont considérées comme des entreprises fédérales. Suivant la parution de ces publicités, le Commissariat a pris note de l'accroissement du nombre de demandes de renseignements sur la *LPRPDÉ*.

Site Web

L'an dernier, le site Web du Commissariat a fait l'objet d'une reconception en profondeur et a été beaucoup élargi afin de donner suite au mandat de sensibilisation du public à la nouvelle *Loi*.

De nombreux efforts ont été déployés afin d'assurer que le site Web soit une ressource à jour concernant la protection des renseignements personnels ainsi qu'un outil de recherche utile sur les questions liées à la vie privée. En bout de ligne, le site Web de facture nouvelle est plus interactif, convivial et pertinent à la fois pour les individus et les entreprises.

Je suis heureux d'indiquer que le site Web est un outil de plus en plus efficace pour joindre les Canadiens et les Canadiennes et d'autres personnes, et sert à les renseigner sur les questions liées à la vie privée. Le nombre de visites du site continue d'augmenter, qui s'élève en moyenne à 11 500 par mois.

Activités de communication

1er janvier 2001 - 30 novembre 2001

Activité		Nombre
Allocutions prononcées par le Commissaire à la protection de la vie privée		35
Allocutions prononcées par les cadres supérieurs		31
Communiqués		15
Entrevues avec les médias		210
Documents distribués		**27 586**
Guide à l'intention des entreprises	13 005	
Guide à l'intention des citoyens	8 707	
Autres (rapports annuels, signets, feuilles de renseignements, lois, etc.)	5 874	
Nombre moyen de visites du site Web par mois		11 500

Troisième partie
Services de gestion

Préparatifs pour la mise en œuvre de la loi pour le secteur privé

Le Commissariat a ajouté à son personnel et accru son budget pour se préparer à la mise en œuvre de la *Loi sur la protection des renseignements personnels et les documents électroniques*, qui est entrée en vigueur le 1er janvier 2001.

Notre budget a été augmenté, passant à plus de 11 millions de dollars par année à compter du 1er avril 2001; il était de 8,7 millions durant l'exercice 2000-2001. Cette augmentation budgétaire permettra au Commissariat d'apporter de nombreux changements importants, y compris les suivants :

- accroître le personnel affecté aux demandes de renseignements afin de pouvoir répondre aux appels plus nombreux;
- prolonger les heures d'affaires, de 9 h à 17 h, dans tous les fuseaux horaires du Canada;
- établir la Direction des Examens et des pratiques en matière de protection des renseignements personnels, qui se chargera des vérifications aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques* et qui poursuivra le travail effectué dans le secteur privé;
- établir la Direction des communications et des analyses stratégiques, qui se chargera de l'actuelle fonction de recherche, de façon à focaliser les communications et la sensibilisation du public et à faire en sorte que nous soyons un centre de connaissances spécialisées sur les questions relatives à la vie privée;
- ajouter au nombre d'enquêteurs qui traiteront les plaintes aux termes des deux lois.

Un cadre financier à long terme touchant le financement futur sera présenté au Secrétariat du Conseil du Trésor du Canada en 2003-2004.

Ressources

(1er avril 2000 - 31 mars 2001)

	ETP	Dépenses globales	Pourcentage du total
Vie privée	56	7 418 451 $	89 %
Services de gestion	10	941 369 $	11 %
Total	**66**	**8 359 820 $**	**100 %**

Nota : Par ETP, on entend « équivalent temps plein » ou le personnel à temps plein.

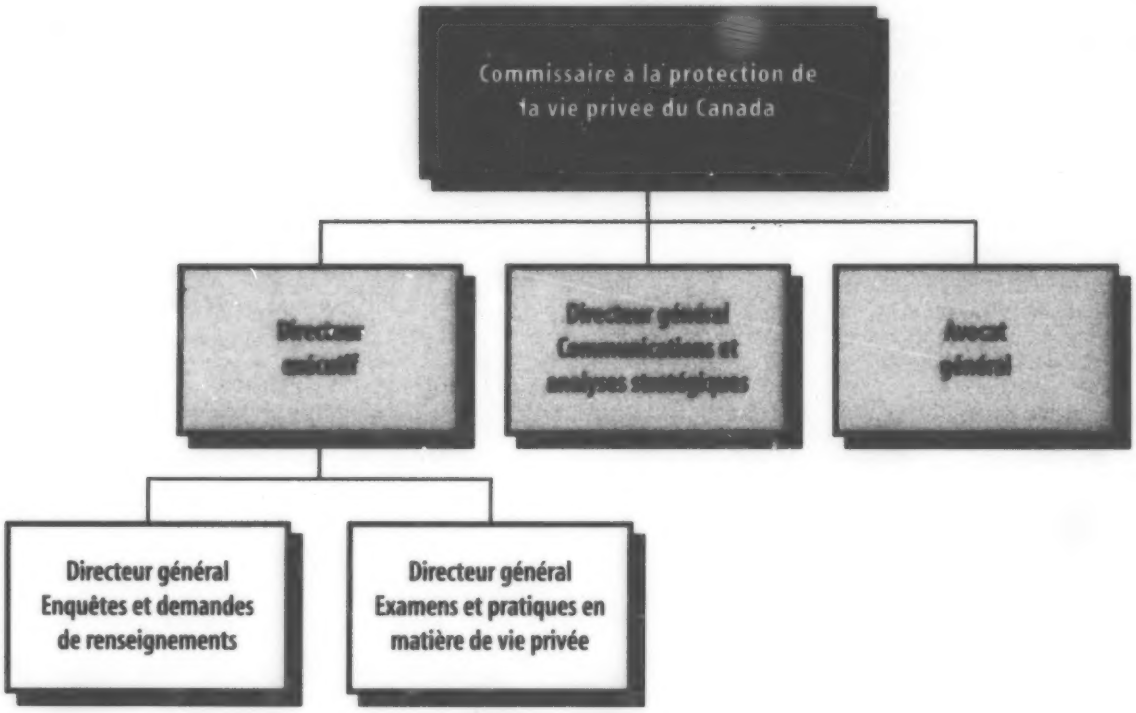
Dépenses détaillées[1]
1er avril 2000 - 31 mars 2001

	Vie privée	Services de gestion[2]	Total
Salaires et traitements	3 776 280 $	464 091 $	4 240 371 $
Cotisations au régime d'avantages sociaux des employés	611 000	84 500	695 500
Transports et communications	268 588	93 470	362 058
Information	979 136	1 993	981 129
Services professionnels	600 427	121 197	721 624
Location	33 036	13 958	46 994
Réparations et entretien	327 711	32 721	360 432
Matériel et fournitures	62 616	28 400	91 016
Acquisition de machines et d'équipements	759 403	100 998	860 401
Autres subventions et paiements	254	41	295
Total	**7 418 451 $**	**941 369 $**	**8 359 820 $**

Nota :

[1] Les dépenses ne comprennent pas les redressements finals de fin d'exercice.

[2] Les dépenses des Services de gestion sont également partagées entre le Commissariat à la protection de la vie privée du Canada et le Commissariat à l'information du Canada.

Structure organisationnelle

Commissariat à la protection de la vie privée du Canada